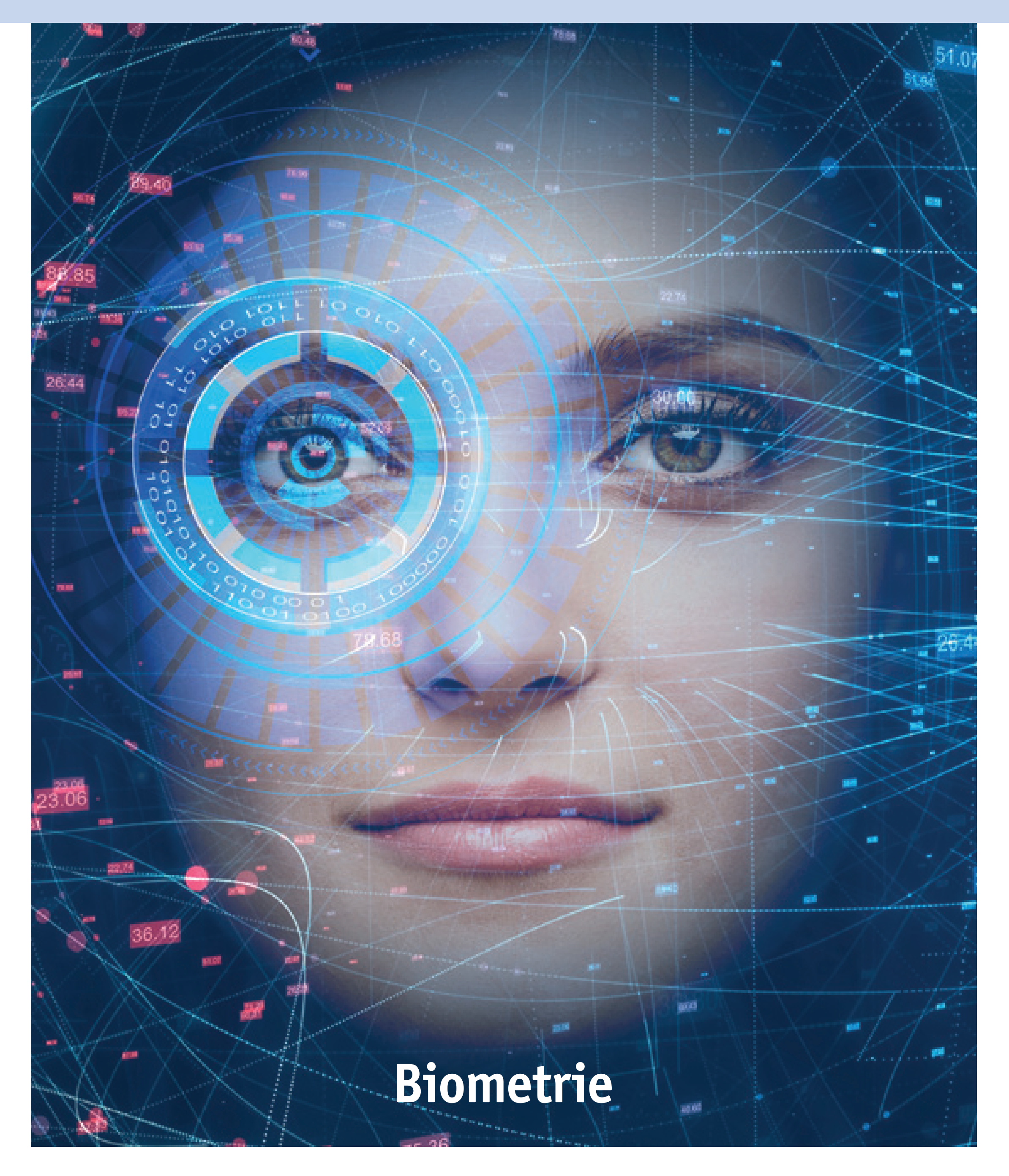
1/2021

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

44. Jahrgang
ISSN 0137-7767
14,00 Euro



Biometrie

■ Gesichtserkennung im Alltag ■ Stimm- und Spracherkennung – Fluch und Segen der Zukunft ■ Systeme biometrischer Identifizierung ■ Stempeluhren mit Fingerabdruck-Scanner ■ Widerstand gegen Entschlüsselungspläne des EU-Rats ■ #PrivacyIsNotACrime ■ Pressemitteilungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Foto: Pixabay..com

20./21. April 2021
FFD Forum für Datenschutz:
„Datenschutztage 2021 – Der praxisorientierte Datenschutz-Kongress“
Mainz

23. April 2021
EAID-Tagung „Neue Herausforderungen für die Konzeption von Datenschutz und Informationsfreiheit“
Europäische Akademie Berlin

01. Mai 2021
Redaktionsschluss DANA 2/2021
Schwerpunkt: Bildung

19.-21. Mai 2021
BvD-Verbandstage & Behördentag „Nextlevel Datenschutz – Der Datenschutzbeauftragte als Lotse in der Digitalisierung“
BvD e.V., online

14./15. Juni 2021
Computas: „DuD 2021 - Datenschutz und Datensicherheit“,
23. Jahresfachkonferenz
Berlin

DANA
Datenschutz Nachrichten
ISSN 0137-7767
44. Jahrgang, Heft 1

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Dr. Thilo Weichert
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autorinnen und Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 14 Euro. Jahresabonnement 48 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, Pixabay, AdobeStock, shutterstock, iStock

Editorial


Bild: iStock.com/ismagilov

Digitalisierung first – Bedenken second. Dieser knackige frühere Wahlkampfslogan der FDP scheint – so sinnbefreit er sein mag – in Politik und Medien immer populärer zu werden. Es geht um den Schutz der Gesundheit angesichts der Coronapandemie, um die Effektivierung der Verwaltung, um weniger Bürokratie, immer wieder um Sicherheit. Derzeit wird die Sicherheit für Schwache, wie Alte, Kinder, Kranke und digital Unbedarfte, als Argumentationsmuster bevorzugt. Datenschutzbedenken bleiben „second“ und fallen dann oft hintunter. Die DANA versucht mit ihren Meldungen und dem Abdruck von Pressemitteilungen die vielen Baustellen zu dokumentieren, auf denen derzeit mehr oder weniger bedenkenfrei digitalisiert wird.

Als Schwerpunkt dieses Heftes haben wir „Biometrie“ gewählt (dies war zuletzt im Heft 2/2004 der Schwerpunkt). Der konkrete Anlass, dieses Thema, das praktisch in jeder DANA zumindest in den Meldungen vertreten ist, stärker hervorzuheben, war die erfolgte Änderung des Personalausweisgesetzes, die uns ab August 2021 zur Abgabe unserer Fingerabdrücke beim Beantragen eines Ausweises verpflichtet.

Dass dies aber nur ein Baustein eines viel größeren Überwachungstrends ist, das zeigt uns die gesetzliche Bestandsaufnahme zum Einsatz von Fingerabdrücken und automatisiert auswertbaren Gesichtsbildern insbesondere im Flüchtlingsbereich (Weichert), die gesellschaftliche Etablierung der Gesichtserkennung (Neumann) sowie der sog. Sprachassistenten (Holzgraefe) im Alltag. Der Datenschutz hat immer wieder Gerichte auf seiner Seite, so nun auch das Landesarbeitsgericht Berlin-Brandenburg in Sachen Biometrie am Arbeitsplatz.

Die nächste Ausgabe der DANA, das Heft 2/2021, wird sich schwerpunktmäßig mit der Digitalisierung im Bildungsbereich befassen – ein Dauerbrenner in der aktuellen Debatte. Das Heft 3/2021 soll sich dem eGovernment widmen, also dem Einsatz von Informationstechnik in der Verwaltung. Anregungen aus der DANA-Leserschaft zu diesen Schwerpunkten sind willkommen.

Autorinnen und Autoren dieser Ausgabe:

Susanne Holzgraefe
Vorstandsmitglied in der DVD, holzgraefe@datenschutzverein.de, Bielefeld

Hans-Dieter Neumann
Datenschutzauditor und Datenschutzbeauftragter (TÜV-cert),
hans-dieter.neumann@posteo.de, Hamburg

Thilo Weichert
Vorstandsmitglied in der DVD, Mitglied im Netzwerk Datenschutzexpertise,
weichert@datenschutzverein.de, Kiel

Hans-Dieter Neumann

Gesichtserkennung im Alltag

Wenn das Gesicht zur Wanze wird


Bild: iStock.com/Prostock-Studio

Als am 13. Oktober 1970 das erste Datenschutzgesetz der Welt in Kraft trat – es war der Vorläufer des Hessischen Landesdatenschutzgesetzes – sagte der damalige Ministerpräsident Albert Oswald: „Die Orwellsche Vision des allwissenden Staates, der die intimsten Winkel menschlicher Lebenssphäre ausforscht, wird in unserem Land nicht Wirklichkeit werden.“[1] Da mag man doch gleich ein anderes Zitat des Soziologen Dirk Baecker gegenüberstellen: „Wir haben es mit nichts Geringerem zu tun als mit der Vermutung, dass die Einführung des Computers für die Gesellschaft ebenso dramatische Folgen hat wie zuvor die Einführung der Sprache, der Schrift und des Buchdrucks.“[2]

Heute sehen wir uns mit Entwicklungen konfrontiert, mit denen vor 50 Jahren sicherlich nicht zu rechnen war. Wenn wir Plätze überqueren, Ladengeschäfte betreten oder mit öffentlichen Verkehrsmitteln fahren, werden wir mehr oder weniger intensiv mit Instrumenten zur Überwachung konfrontiert.[3] Eine hochaktuelle Entwicklung von besonderer Bedeutung dabei ist die Gesichtserkennung, genauer die automatische Gesichtserkennung.

Der erste Rechtfertigungsgrund für den Einsatz von Überwachungssoftware ist in der Regel ein vermuteter oder unterstellter Sicherheitsbedarf. Der Schutz der Bevölkerung vor terroristischen Angriffen liefert die Rechtfertigung für den Einsatz, und mit ihm beginnt die Verbreitung. Innenminister Seehofer plant rund 100 Bahnhöfe und einige Flughäfen mit Kameras zur Gesichtserkennung auszustatten.

Gesundheit

Auch das Argument Schutzbedarf im Gesundheitswesen wird von der Gesellschaft akzeptiert und für den Einsatz herangezogen. Gerade in der jetzigen Pandemiezeit zeigen sich die Innovationsschübe im Bereich der künstlichen Intelligenz besonders hoch. In Nachrichtensendungen über die Belastung italienischer Spitäler konnten an den Eingängen Erfassungsgeräte beobachtet werden, die inzwischen auch in Deutschland auf dem Markt sind.

Die etwa handygroßen Geräte werden eingerichtet, um die Körpertemperatur der Besucherinnen und Besucher zu erfassen und bei ungünstiger Disposition den Zugang zur Klinik oder zur Pflegeeinrichtung zu verweigern. Allerdings können diese Geräte auch bei entsprechender Schaltung bis zu 22.400 Gesichter oder besser gesagt, die extrahierten biometrischen Daten der Gesichter, speichern. Die Kapazitäten beim Einsatz von Servern vervielfältigen sich entsprechend.

Es liegt fast schon auf der Hand, dass auch Stadien, Universitäten, Theater, Flughäfen und viele andere Einrichtungen einen solchen Schutz für sich beanspruchen. Und so „diffundieren“ diese intelligenten Videokameras durch unsere Gesellschaft, bis sie wie selbstverständlich an fast jeder Ecke zu finden sind und offensichtlich auch große Teile der Gesellschaft nicht mehr stören. An prominenten Orten können die klassischen Videokameras unbemerkt von Passanten durch solche mit Gesichtserkennungssoftware ausgetauscht werden, wodurch sie in die Lage versetzt werden, nicht nur Verkehrsströme zu beobachten, sondern auch die Nummernschilder der Fahrzeuge sowie die Fahrzeuginsassen zu erfassen. Im Gespräch ist zum Beispiel, die Erfassungsstellen für Mautgebühren durch eine diesbezügliche Videoüberwachung zu ergänzen.

Komfort

Die Vorteile für die Unternehmen liegen auf der Hand: Mit Software zur automatischen Gesichtserkennung können Gäste in Hotels sofort mit Namen empfangen werden. Im Handel können Kundinnen und Kunden mit ihrem Gesicht und einer zusätzlich eingegebenen Telefonnummer Rechnungen begleichen, und der Schaffner im Zug kann Tickets der Reisenden auf Gültigkeit hin überprüfen. Die Post rüstet Shops mit Gesichtserkennung aus und will damit personalisierte Werbung auf einem Display präsentieren. Die Anwendungs-

möglichkeiten scheinen keine Grenzen zu kennen.

Aber auch die Verbraucher genießen offensichtlich die mit dieser Form der Datenerfassung verbundenen Bequemlichkeiten. Wo früher Besucher einen Chip in ihrem Unterarm auslesen ließen, um Eintritt in den VIP-Club zu bekommen, reicht heute ein Blick in die Kamera am Eingang. Die neuen Mobilfunktelefone fast aller Hersteller sind per Gesichtserkennung einschaltbar.

Immer mehr Kraftfahrer verwenden umfassende Systeme der Datenerfassung für ihr Auto, zumal der BGH die eigentlich verbotenen Dashcams nun doch als Nachweis zur Beweissicherung gestattet hat.[4] In diesem Segment tut sich der US-amerikanische Hersteller Tesla besonders hervor.[5] Die Fahrzeuge haben bis zu acht Kameras an Bord und speichern ein umfassendes Datenmaterial (nicht nur der Kameras). Wo werden diese Daten gespeichert? Im Fahrzeug beim Halter? In einer Vertragswerkstatt? Oder doch beim Hersteller? Die uns hier bewegenden Fragen beziehen sich auf die grundlegenden Rechte der betroffenen Personen. Wo zum Beispiel kann der Auskunftsanspruch nach Art. 15 DSGVO geltend gemacht werden? Korrekte Antworten würden u.a. die zuvor gestellten Fragen erübrigen.

Elon Musk gibt im Interview mit Kontraste an, dass die Datenübermittlung vollkommen anonymisiert stattfinde. Damit unterlägen die Daten auch nicht mehr der DSGVO. Doch wenn die Daten im Tesla tatsächlich anonymisiert, also definitiv nicht mehr rückführbar sind, dann stellt sich die Frage, was der Autohersteller auf der anderen Seite des Atlantiks mit diesen Daten noch vorhat.

Schauen wir uns doch noch zwei Sonderfälle der Anwendung an. Neben der kommerziellen Software gibt es inzwischen auch ein großes Angebot an frei verkäuflicher Software zur Gesichtserkennung.[6]

Medienprivileg

Ein Software-Startup beruft sich auf das Medienprivileg seiner Kunden als Rechtsgrundlage und bietet ihnen an, Archive auf Basis der Gesichtserkennung zu erstellen. Fotografen und Journalisten können in solchen Archiven stöbern, um festzustellen, ob zu einem aktuellen Bericht bereits archivierte Aufnahmen vorhanden sind, auf die man evtl. ergänzend zurückgreifen könnte.[7]

Das Unternehmen Lapetus Solutions hat ein Softwareprodukt entwickelt, das Selfies sehr akkurat auswerten kann. Kunden wie Versicherungsunternehmen können in Verbindung mit einigen Angaben zu einem Versicherungsnehmer dessen Gesundheit feststellen und Verträge individuell anpassen. Sogar ein künftiger Todeszeitpunkt soll mittels dieser Software und weiteren Gesundheitsangaben, die oft mit Fragebogen von der betroffenen Person selbst erhoben werden, ermittelt werden können.[8]

Identifizierung

Biometrische Daten sind zur eindeutigen Identifizierung von Menschen geeignet, wenn die gemessenen Merkmale einmalig sind.[9] Diese Merkmale müssen aber nicht zwangsläufig weltweit eindeutig sein. Dies birgt wiederum die Gefahr, dass es zu Ähnlichkeiten und somit auch zu Verwechslungen kommen kann.

Bereits in früheren Untersuchungen wurde von Diskriminierungen durch den Einsatz von biometrischen Verfahren bei polizeilichen Ermittlungen und Strafverfahren berichtet.[10] In einer aktuellen Studie über 189 Algorithmen zur Gesichtserkennung bei 99 Organisationen konnten belastbare Nachweise für fehlerhafte Ergebnisse konkret hinsichtlich Alter, Herkunft und Volkszugehörigkeit herausgearbeitet werden.[11] Der „Missbrauch“ dieser Technologie durch Sicherheitsorgane führte dazu, dass in San Francisco Gesichtserkennung als Waffe eingeordnet und verboten worden ist. Die drei großen Anbieter Amazon, IBM und Microsoft stellen ihre Erkennungssoftware für die Polizei in den USA nicht mehr zur Verfügung.

Terrorbekämpfung

Da nun die Gesichtserkennung immer weiter in der Gesellschaft verankert ist, wird im nächsten Schritt versucht, mit der bekannten Argumentation der Terrorbekämpfung die Überwachung mittels Gesichtserkennung zu intensivieren. Der Berliner Südbahnhof war hierfür ein geeignetes Testfeld. In Zeiten der Pandemie muss, analog zu den Schutzansprüchen der Sicherheitsorgane, die Software nun auch Gesichter erkennen, die sich hinter Masken verbergen. Die Produkte dafür sind schon im Markt. Maskenträger können mit fast 100-prozentiger Sicherheit erkannt werden.[12]

Es stellt sich die Frage, wie die Zukunft der künstlichen Intelligenz, speziell mit der automatischen Gesichtserkennung, aussehen kann. Denkbar wäre zum Beispiel, dass Gerichtsverhandlungen im Rahmen der digitalen Zivilprozessordnung (§ 128 ZPO) geführt werden können und alle Akteure über ihr Gesicht eindeutig zu identifizieren sind. Der unternehmerischen Phantasie werden letztendlich nur durch eine durchsetzungsstarke Datenschutzgesetzgebung Grenzen gesetzt. Und so bleibt derzeit nur auf das Zitat von Dirk Baecker zu Beginn dieses Artikels zu verweisen.

1 https://magazin.spiegel.de/EpubDelivery/spiegel/pdf/43176393 (Abruf 31.01.2021).

2 Dirk Baecker: Studien zur nächsten Gesellschaft, Suhrkamp 2007, 4. Umschlagseite.

3 Katharina Nocun, Die Daten, die ich rief; Bastei Luebbe, Köln 2018, S. 22 f.

4 BGH Urteil v. 15.05.2018 – VI ZR 233/17.

5 https://www.daserste.de/information/politik-weltgeschehen/kontraste/videosextern/verstoesst-tesla-systematisch-gegen-datenschutzregeln-104.html

6 https://www.freeware.de/programme/gesichtserkennung/ (Abruf 31.01.21).

7 Telefonat am 31.01.2021 mit Eugen Gross, CEO der Firma auconix.ai.

8 https://computerwelt.at/news/selfies-versicherungen-errechnen-todeszeitpunkt/ (Abruf 31.01.21).

9 Weichert in Kühling / Buchner: DS-GVO / BDSG, Art. 14, Rn 2.

10 Weichert, Staatliche Identifizierung durch Biometrie, DANA 2/2004, S. 9 ff.

11 https://www.theverge.com/2019/12/20/21031255/facial-recognition-algorithm-bias-gender-race-age-federal-nest-investigation-analysis-amazon (Abruf 31.01.21).

12 https://www.heise.de/hintergrund/Gesichtserkennung-fuer-Maskentraeger-5038656.html (Abruf 31.01.21).

Susanne Holzgraefe

Stimm- und Spracherkennung – Fluch und Segen der Zukunft

Fast dreißig Jahre waren vergangen, seit meine Freundin Kerstin und ich uns aus den Augen verloren hatten. Unser altes Gymnasium hatte alle Ehemaligen zu einer Jubiläumsfeier eingeladen. In Nostalgie schwelgend gab ich die Namen einiger alter Schulfreunde in die Suchmaschine ein. Erstaunlicherweise stand meine alte Freundin Kerstin im Telefonbuch. Ich zögerte nicht, ich nahm das Telefon und rief sie an. „Kerstin?" fragte ich, nachdem am anderen Ende eine Frauenstimme abnahm. „Susanne!" rief sie erfreut „Was für eine Überraschung." „Woher weißt Du, dass ich das bin?" fragte ich erstaunt. „Deine Stimme würde ich immer und überall erkennen." Wow! Und das nach so langer Zeit. Ich war beeindruckt. Aber tatsächlich hatte auch ich ihre Stimme sofort erkannt. Ähnlich ging es mir mit den Stimmen meiner anderen alten Schulkameraden, die ich dann auf der Jubiläumsfeier traf. Einige von uns haben sich gegenseitig tatsächlich nur an der Stimme wiedererkannt und nicht am Aussehen.

Weitere Situationen zeigen, wie stark wir auf eine gegenseitige Identifizierung anhand der Stimme geprägt sind. Ein klassisches Beispiel sind reine Audio- bzw. Telefonkonferenzen. Nach wenigen Worten erkennen sich viele Teilnehmenden gegenseitig an der Stimme.

Verwirrung tritt manchmal bei Synchronsprechern ein, die ihre Stimme mehreren Schauspielern geben. Ich höre im Nebenzimmer, dass mein Mann im Wohnzimmer einen Film schaut. Anhand der Stimmen, die ich erkenne, wundere ich mich, dass er diesen Film schaut. Doch als ich die Bilder sehe, stelle ich fest, es ist ein ganz anderer Film mit ganz anderen Schauspielern; eine oder mehrere Schauspieler sind lediglich von denselben Stimmen wie im von mir vermuteten Film synchronisiert worden.

Neben menschlichen Stimmen können wir durchaus auch die Stimmen von einzelnen Tieren unterscheiden. So hat jede Katze ihre eigene, individuelle Stimme.

Eine Erklärung, warum viele Menschen gut darin sind, andere Menschen an der Stimme zu erkennen, mag darin liegen, dass anhand der Stimme oft selbst Freunde von Feinden unterschieden werden.

Ist die Stimme eines jeden Menschen einzigartig?

Sind Ihnen schon mal zwei Menschen begegnet, deren Stimmen sich exakt identisch anhörten? Kennen Sie jemanden, dem schon mal zwei Menschen mit identischer Stimme begegnet sind? Obwohl ich jährlich viele Menschen neu kennenlerne, sind mir tatsächlich noch nie zwei Menschen begegnet, deren Stimmen ich verwechseln könnte.

Wenn mir Personen erzählt haben, dass sie Menschen anhand der Stimme verwechselt haben, war dies zumeist im Zusammenhang mit der Tatsache, dass sie auf einen Parodisten reingefallen sind, der Stimmen berühmter Persönlichkeiten nachahmte. Geübte Ohren hören aber sofort den Unterschied. Selbst wenn das menschliche Ohr versagt, so zeigen Messgeräte durchaus Unterschiede.

Aber, nur weil mir und vielleicht Ihnen noch nie zwei Menschen begegnet sind, die eine identische Stimme hatten, ist das noch lange kein Beweis, dass die Stimme eines Menschen so eindeutig ist, dass sich dadurch jeder Mensch eindeutig identifizieren lässt. Immerhin lassen sich in der Judikative und Exekutive Fälle finden, bei denen Sprach- und Stimmerkennung als Beweismittel zugelassen wurden.

Jeder Mensch hat eine eigene Art zu sprechen. Menschen reden verschieden schnell, haben eine höhere oder tiefere Stimme. Auch beim Dialekt und der Wortwahl hört man Unterschiede. Außerdem hat jeder kleinere oder größere Sprachfehler. Die Kombination dieser Eigenschaften macht einen Sprecher fast unverwechselbar. Deshalb dient die Stimme in Kriminalfällen auch als Beweismittel für die Identität eines Täters (Stuttgarter Zeitung v. 17.12.2015).[1]

Die menschliche Stimme und die Technik

Bevor Alexander Graham Bell das Telefon erfand, forschte er zum Thema menschliche Stimme. Darüber hinaus war es Bell, der Schallübertragung in einem Lichtstrahl erfand,[2] was wohl die Grundidee für die heutige Kommunikationsübertragung mit Hilfe von Lichtfaserkabeln lieferte.

Das Übertragen möglichst nur des Frequenzbereichs der menschliche Stimme und keiner weiteren Geräusche, wie Wind, Autobahnlärm oder anderer Nebengeräusche, das beschäftigt Telefonie, Radio sowie Film- und Fernsehen schon seit langer Zeit; die Audiotechnik wird in diesem Bereich immer weiter perfektioniert.

Darüber hinaus findet für verschiedenste Zwecke eine stetige Weiterentwicklung von Filtern statt, die eine Stimme bzw. eine aufgezeichnete Stimme so aufbereiten, dass sie, selbst wenn sie verzerrt oder technisch verändert wurde, sich am Ende doch einer einzelnen Person zuordnen lässt.

Nicht nur Polizei und Staatsanwaltschaft haben hieran ein großes Interesse, sondern auch Unternehmen, die Stimm- und Sprachsteuerungen für ihre Geräte anbieten. Die bekanntesten sind wohl Apple und Google, die es ermöglichen, dass ihre Smartphones und andere Geräte per Spracheingabe gesteuert werden. Durch anfängliche Konfiguration erkennen die Geräte mittlerweile schon ziemlich genau, ob ein zugelas-

sener Nutzer einen Steuerbefehl spricht oder jemand anderes.

Alexa (Amazon) erkennt, welches Familienmitglied den Befehl gesprochen hat und bietet dem Familienmitglied dann ein auf dieses personalisiertes abgestimmtes Programm an. Zum Beispiel werden dem einen Kind, das zwei Piratenhörbücher gehört hat, weitere Hörbücher mit Piratengeschichten angeboten und dem anderen Kind Detektivgeschichten, da die eingebaute künstliche Intelligenz aus dem gestrigen Hören der *Drei Fragezeichen* geschlossen hat, dass das Kind auf Detektivgeschichten steht.

Auch Siri (Apple) und Google Home erkennen anhand der Sprache, ob es sich um einen vorher konfigurierten und damit legitimierten Benutzer handelt; wenn nicht, werden die Sprachbefehle ignoriert.

Sprach- und Stimmerkennung als Zugangsmittel sind heutzutage bereits an vielen Stellen gang und gäbe. Die Automobilindustrie arbeitet an Entwicklungen, mit denen sich zukünftig Autos per Spracheingabe steuern lassen. Das gesprochene „Sesam öffne Dich" und die Tür öffnet sich ist längst keine Zukunftsmusik mehr. Hierbei öffnet sich die Tür nicht, weil Sie das richtige Codewort gesagt haben, sondern vor allem, weil die Technik in der Tür Sie anhand Ihrer Stimme, Ihrem Dialekt und ein paar anderen Merkmalen, die die Technik aus den drei gesprochenen Worten entnehmen konnte, als Ali Baba erkannt hat.

Die Technik macht weitere Fortschritte. Fehlerarme Identifizierung einzelner Personen „on air" ist heutzutage z.B. auch mit Hilfe von Geruchssensoren möglich.

Ist die menschliche Stimme hackbar?

Ein chinesisches Sprichwort sagt: „Wer einen Schatz hat, sollte mit Dieben rechnen." Wenn wir über Sprach- und Stimmerkennung reden, reden wir über Sender und Empfänger. Der Sender ist der Sprechende und der Empfänger ist das Ohr oder eine technische Einrichtung, die anhand von Messtechnik und künstlicher Intelligenz versuchen den Sprechenden eindeutig zu identifizieren.

Mit Sprachtechnik lässt sich die Audiotechnik überlisten. Eine menschliche Stimme kann heute auf technischem Wege so imitiert werden, dass damit Sprach- und Stimmerkennungssensoren überlistet werden. Ein Hacker könnte damit die Stimme eines berechtigten Benutzers technisch nachstellen, um dessen Smartphone oder dessen Alexa zu steuern oder den Zugang zu vertraulichen Räumlichkeiten zu erschleichen. Frei nach dem Motto: Kaum ist die Technik auf dem Markt, ist sie auch schon nicht mehr sicher.

In neuster Technik wird, wie oben dargestellt, Sprach- und Stimmerkennung mit Geruchssensorik kombiniert, um so Hackern den Weg doch zu versperren.

Rechtliche Grundlagen zur menschlichen Stimme

Stimmaufzeichnungen, die zur Identifizierung genutzt werden können, zählen als biometrische Daten zu den besonderen Kategorien personenbezogener Daten der Datenschutz-Grundverordnung (DSGVO).[3] Das bedeutet, dass eine Verarbeitung generell untersagt ist, es sei denn, es liegt eine der in Art. 9 Abs. 2 DSGVO aufgeführten Ausnahmen vor.

Ergänzend ist anzumerken, dass die DSGVO und das Bundesdatenschutzgesetz (BDSG) keine Anwendung finden, wenn die Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten verarbeitet werden.[4] Klassische Beispiele hierfür sind Türsprechanlagen und Babyphones, die über keinerlei Speicherung verfügen.

Lange vor der DSGVO erkannte die deutsche Gesetzgebung, dass die Bevölkerung vor Audioüberwachung geschützt werden sollte. Der Einsatz von Wanzen und anderen Abhörgeräten zur Bespitzelung ist verboten. § 201 Strafgesetzbuch (StGB) befasst sich mit der Verletzung des vertraulich gesprochenen Wortes.

Videoüberwachung ja, Audioüberwachung nein?

Videoüberwachung ist im Datenschutz ein häufig diskutiertes Thema. Was aber ist mit Audioüberwachung? Schon kostengünstige Webcams haben in der Regel eingebaute Mikrofone, mit denen sich gesprochene Worte problemlos aufzeichnen lassen. Derartige Webcams kommen zum Beispiel an Tankstellen für Überwachungszwecke zum Einsatz. Ist ein erstellter Audiomitschnitt zulässig und darf ein solcher zur Ermittlung des Straftäters verwendet und vor Gericht verwertet werden? Dem Aufzeichnenden könnte ein Audiomitschnitt sehr schnell gegenüber Richtern oder gegnerischen Anwälten zum Verhängnis werden, wenn § 201 StGB verletzt wurde. Ist eine Videoüberwachung zulässig, so ist eine Audioüberwachung nicht automatisch auch zulässig. Es ist ratsam, darauf zu achten, dass die Kameras keine Mikrofone haben und generell, dass keine Mikrofone lauschen.

Audioüberwachung durch Alexa oder Siri

Alexa und andere vergleichbare Geräte lauschen durchgehend, um per Sprache aktiviert werden zu können. Sprach- und Stimmerkennungs-Intelligenz sorgt dafür, dass sie, selbst wenn mehrere Menschen durcheinander sprechen, die Befehle ihrer legitimierten Benutzer erkennen und die anderen ignorieren. Ignorieren sie aber wirklich alle anderen? Werden die gesprochenen Worte an den Hersteller gesendet und ausgewertet?

Apple versichert, dass die Auswertung der Daten, die *Hey Siri* beim Lauschen aufgreift, ausschließlich lokal verarbeitet werden. Die Lauschaufnahmen würden kontinuierlich überschrieben. Und in keinem Fall nähmen die Geräte Gespräche auf und sendeten diese an das Unternehmen, bevor Siri in Aktion tritt.[5]

Alexa hingegen schickt die Sprachkommandos zur Auswertung an die Amazon Cloud und speichert sie dort.[6] Wenn Alexa ein Sprachkommando erkennt, schickt es das an die Cloud. Was ist aber mit allen anderen Wortfetzen, die es beim Lauschen aufgreift? netzpolitik.org schreibt hierzu:

Der Smart Speaker lauscht im Hintergrund auf alle Gespräche. Glaubt man Amazon, werden nur Ausschnitte, die die Software als Befehl erkennt, an die Server des Unternehmens weitergeleitet.[7]

Der Artikel von netzpolitik.org macht deutlich, wie schnell Amazons Alexa zu dem Schluss kommen kann, es habe ein Sprachkommando gehört. Gemäß meinen eigenen Erfahrungen ist auch Apples Siri nicht perfekt, wenn es mich völlig unerwartet anspricht: „Ich habe Dich nicht richtig verstanden." Was bzw. welche Worte genau Siri getriggert haben zu reagieren bleibt häufig unklar. Dass die Technik hier noch in den Kinderschuhen steckt, wird in solchen Momenten sichtbar.

Datenschutzrechtlich stellen sich einige interessante Fragen:

Greifen DSGVO und BDSG überhaupt und wer ist verantwortlich?

DSGVO und BDSG sind nicht anwendbar, wenn natürliche Personen die Daten ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeiten verarbeiten. Relevant ist also zunächst, ob der Betreiber des Gerätes eine natürliche Person ist. Wird Alexa zum Beispiel im Kindergarten, in einem Unternehmen oder in einer Behörde eingesetzt, so ist der Betreiber keine natürliche Person. Sowohl DSGVO als auch BDSG und ggf. auch die Datenschutzbestimmungen der Länder finden Anwendung. Die vollumfängliche Verantwortung liegt beim jeweiligen Betreiber.

Wie aber ist das bei privaten Haushalten?

Besteht ein Haushalt lediglich aus einer einzelnen Person, so ist der Betreiber eine natürliche Person. Ausschlaggebend ist dann, ob die Daten ausschließlich zur Ausübung persönlicher und familiärer Tätigkeiten verarbeitet werden. Fällt darunter auch die Verarbeitung, wenn mehrere Personen zusammen wohnen? Ob das Datenschutzrecht vollumfänglich Anwendung findet, hängt im Zweifel stark vom Einzelfall und dessen richterlicher Bewertung ab. Ob eine einzelne Person der Gemeinschaft bzw. Familie vollumfänglich verantwortlich ist oder alle Mitglieder der Familie bzw. der Gemeinschaft gemeinsam verantwortlich sind, ist von der Familie bzw. der Gemeinschaft und deren internen Strukturen und Absprachen abhängig.

Werden die Daten denn ausschließlich zur Ausübung von persönlichen und familiären Tätigkeiten verarbeitet? Auch insofern besteht ein richterlicher Beurteilungsspielraum je nach Einzelfall. Wie schon erwähnt, ist es bei Türsprechanlagen oder Babyphonen, bei denen keine Daten gespeichert und die Daten auch sonst nicht aufgezeichnet werden, offensichtlich, dass die Informationen nur für den persönlichen und familiären Zweck verwendet werden.

Fraglich ist es jedoch bei Geräten, die Audioaufzeichnungen erstellen. Wo werden die Daten gespeichert? Alexa und Siri speichern die Worte, die sie beim Lauschen aufgreifen. Die Hersteller beider Systeme beteuern, dass sie die beim Lauschen aufgegriffenen Worte zur Ermittlung, ob es sich um ein legitimiertes Kommando handelt, lediglich lokal auf dem Gerät zur Auswertung speichern. Apple versichert darüber hinaus sogar, die Daten lokal kontinuierlich unverzüglich zu überschreiben.

Ältere Geräte bzw. Geräte, die keine neueren Software-Updates installiert haben, können Sprach- und Stimmerkennung eventuell noch gar nicht personalisiert auswerten. Egal wer „Hey Siri" oder „Alexa" ruft, kann damit ein Kommando auslösen. Neuere Geräte bzw. Software reagiert nur noch, wenn „Hey Siri" bzw. „Alexa" von einer vorher konfigurierten, bestimmten Person gerufen wird. Bei Alexa kann für jedes Familienmitglied ein eigenes Profil angelegt werden. Beide Konzerne entwickeln ihre Technik stetig weiter. Es soll vermieden werden, dass z.B. die Apple-Geräte aller Bahnreisenden mit einer Musikwiedergabe beginnen, wenn ein Fahrgast ruft: „Hey Siri, spiele Helene Fischer."

Mit personalisierten Zugängen lassen sich natürlich auch Inhalte besser zuordnen und damit kontrollieren. Kinder könnten nur für altersgerechte Filme freigeschaltet werden. Was die individuelle Profilbildung der einzelnen Benutzer angeht, ist Alexa sehr bestrebt.

Wäre die Technik bereits so weit, dass die Kommando-Erkennung perfekt personalisiert funktioniert, wäre eine Auswertung zu rein persönlichen und familiären Tätigkeiten auf den ersten Blick erkennbar. Bis es aber soweit ist, müssen Apple oder Amazon noch an der Technik feilen. So schreibt heise online:

Die Spracherkennung von Alexa lernt durch Interaktion mit dem Nutzer ständig dazu und erkennt dessen Stimme schrittweise immer besser.[8]

Auch Siri ordnet immer mal wieder Kommandos durch gesprochene Worte falsch zu.

Das bedeutet, dass sowohl Alexa als auch Siri immer mal wieder Daten Dritter verarbeiten. Die Server, auf denen die Verarbeitung letztendlich erfolgt, können hierbei auf der gesamten Welt stehen. Diese Verarbeitung durch Apple oder Amazon erfolgt nicht „zur Ausübung ausschließlich persönlicher und familiärer Tätigkeiten". Die Verarbeitung dürfte regelmäßig in Drittländern ohne angemessenen Datenschutz erfolgen.

Welche Maßnahmen sollten ergriffen werden?

Kindergärten, Unternehmen, Behörden und andere juristische Personen sollten in ihren Organisationen vorerst den Einsatz von Alexa und Siri vermeiden; zumindest bis die Stimm- und Spracherkennung zuverlässiger und fehlerfreier funktioniert. Hinzu kommen zu berücksichtigende Aspekte aus dem Arbeitsschutz und dem Beschäftigtendatenschutz. Transparenzpflichten gemäß der DSGVO sind einzuhalten. Die Prozesse sind im Verzeichnis der Verarbeitungstätigkeiten aufzunehmen.

Werden Amazons Alexa oder Apples Siri in privaten Haushalten betrieben, so sollten Besucher in jedem Fall beim Betreten des Haushaltes auf die Existenz der Geräte aufmerksam gemacht werden, so dass sie die Möglichkeit haben, frei zu entscheiden, ob sie den Haushalt betreten möchten oder nicht. Das gilt auch für Handwerker, Pflegedienstmitarbeitende, Beschäftigte vom Jugendamt und viele weitere. Die andere Möglichkeit ist die Geräte während der gesamten Dauer des Besuchs zu deaktivieren.

Handwerker, Pflegedienste usw. können bei der Auftragsvergabe schriftlich die Deaktivierung derartiger Geräte für die Dauer der Ausführung vertraglich verabreden. Das legt der Beschäftigtendatenschutz nahe.

Die Ansage, „Zu Dir komme ich nicht, wenn Du Deine Alexa nicht abstellst." gegenüber Alexa-Nutzern hat noch eine

ganze Weile im Familien-, Freundes- und Bekanntenkreis eine Berechtigung.

Stimmerkennung in Smartphones, Tablets, Laptops und Autos

Apples Siri ist auf allen Apple-Geräten installiert. „Hey Google" und auch die Sprachsteuerung in Autos funktionieren entsprechend. Egal, auf welchem Smartphone, Tablet oder Laptop, die Sprachassistenten lauschen genauso wie bei Alexa – mit den gleichen Fallstricken. In Autos sind immer häufiger sprachgesteuerte Assistenten eingebaut, die entweder auf Apple-, Google- oder Amazon-Technik beruhen oder ihnen ähnlich sind.

Die eigene Erfahrung zeigt, dass Siri gerne mal im Meeting, am Kaffeetisch mit der Familie oder auch bei der Fahrt mit mehreren Personen im Auto anspringt. „Hey! Stell das sofort ab!" ist dann häufig die angesäuerte Reaktion von anderen. Siri lässt sich auf allen Apple-Geräten in den Einstellungen schnell und einfach deaktivieren. Uhren und Smartphones können in vielen Situationen komplett ausgeschaltet werden, doch werden gerade in beruflichen Meetings Tablets oder Laptops oft benötigt.

Im beruflichen Umfeld ist es deshalb ratsam die Spracherkennung zu deaktivieren. Es ist nicht sichergestellt, dass nicht versehentlich personenbezogene Informationen oder auch Geschäftsgeheimnisse an Server in Drittländern und an die Hersteller übermittelt werden.

Auch im öffentlichen Bereich, in Bahnen, Bussen, Restaurants usw., könnten die Geräte Sprachfetzen Anderer aufgreifen, als Kommando erkennen und an die Server der Hersteller weiterleiten. Im Grunde genügt es nicht die anderen Passagiere und Gäste darauf aufmerksam zu machen, dass eine Sprachassistenz aktiviert ist; von ihnen kann natürlich nicht verlangt werden die Bahn, den Bus, das Restaurant, das Konzert oder das Museum unverzüglich zu verlassen, wenn sie mit dem Audioscan nicht einverstanden sind. Im privaten Bereich bleibt zumeist die Diskussion mit der Familie, Freunden und Bekannten möglich, wenn bei gegenseitigen Besuchen Geräte lauschen: „Mach bitte Handy und Uhr aus, bevor Du rein kommst."

In Autos sind Mitfahrende betroffen. Ob ein Sprachassistent deaktivierbar ist, hängt vom Hersteller ab. Es bleibt die Frage, wer verantwortlich ist: Ist es der Fahrer oder der Halter? Bei Firmenwagen, die auch privat genutzt werden dürfen, ist das ein spannendes Thema, das zu diskutieren hier den Rahmen sprengen würde.

Stimmerkennung in Spielzeug

Die Puppe, der das Kind seine Sorgen anvertraut, die dann über die Server des Herstellers ausgewertet werden, ist keine Zukunftsmusik, sondern Realität.[9] Digitalcourage hat deshalb bereits im Jahr 2015 einen Big Brother Award an die Firma Mattel für ihre „Hello Barbie"-Puppe verliehen.[10]

Spielzeuge, mit dem Kinder regelmäßig abgehört werden und von dem die Daten nicht nur an die Hersteller des Spielzeugs geschickt werden, sondern auch an die Eltern der Kinder, erobern immer mehr die Kinderzimmer. So werden Kinder von klein auf an Überwachung gewöhnt. Die Sprachassistenten werden immer weiter darauf trainiert, Stimme und Sprache besser zu individualisieren. Dass darüber hinaus individuelle Profile erstellt werden, die dann für Marketing gegenüber den Kindern und andere Zwecke genutzt werden, lässt sich nicht ausschließen.

Fazit

Sprach- und Stimmerkennung nimmt in der heutigen Welt immer mehr Raum ein. Zur Identifizierung einer Person werden häufig nicht nur die Stimmmerkmale ausgewertet, sondern auch Dialekt und weitere Sprach- und Sprecheigenschaften der jeweiligen Person. Damit können nicht nur menschliche Ohren überlistet werden, wie Stimmimitatoren in Parodien gerne zeigen, sondern durch Einsatz technischer Mittel auch die lauschende Technik. Deshalb werden Systeme zur Identifizierung heutzutage durch Geruchssensoren ergänzt. Die automatisierte, technische Sprach- und Stimmerkennung als Authentifizierungsmittel steckt noch in den Kinderschuhen. Fehler sind zu häufig, um sie als zuverlässig und sicher bezeichnen zu können.

Sprach- und Stimmerkennung ist zwar schon vielseitig im Einsatz. Mit den damit erlangten Daten wird Forschung betrieben, um die Auswertung und Mustererkennung zu verbessern. Damit einher geht der wenig beruhigende Umstand, dass Daten von einem selbst wie von Dritten an Hersteller und Server in Drittländern zur Auswertung weitergegeben werden.

Datenschutzrechtlich bleibt das Thema spannend. In Deutschland ist die Wahrung der Vertraulichkeit des gesprochenen Wortes auch Gegenstand strafrechtlicher Regulierung; Audioüberwachung kann als Straftat verfolgt werden. Die Anwendung dieser Regelung ist nicht weniger spannend.

1 Stuttgarter Zeitung, 17.12.2015, Artikel von P. Hummel, A. Viciano, M. Catanzaro, E. Tola: https://www.stuttgarter-zeitung.de/inhalt.forensische-phonetik-wenn-die-stimme-vor-gericht-versagt.87131bc1-60d0-465a-83ef-3e37c00b4d10.html.

2 Wie Alexander Graham Bell das Telefon erfand: https://artsandculture.google.com/story/cAJSsxLLgTshIA?hl=de.

3 Art. 9 DSGVO – Verarbeitung besonderer Kategorien personenbezogener Daten.

4 §1 Abs. 1 letzter Satz BDSG und Art. 2 Abs. 2 lit. c) DSGVO.

5 Apples Erklärung gegenüber Techcrunch https://techcrunch.com/2015/09/11/apple-addresses-privacy-questions-about-hey-siri-and-live-photo-features/; auch veröffentlicht auf Heise: https://www.heise.de/mac-and-i/meldung/Hey-Siri-und-Live-Fotos-Apple-kontert-Datenschutzbedenken-2812422.html.

6 Amazon Alexa: so funktioniert der Sprachassistent https://www.heise.de/thema/Amazon-Alexa.

7 Amazon Echo: Alexa sendet Privatgespräch heimlich an Arbeitskollegen https://netzpolitik.org/2018/amazon-echo-alexa-sendet-privatgespraech-heimlich-an-arbeitskollegen/.

8 Amazon Alexa: so funktioniert der Sprachassistent https://www.heise.de/thema/Amazon-Alexa.

9 siehe DANA 1/2017, S. 42.

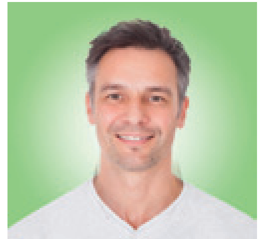
10 Big Brother Award für „Hello Barbie" https://bigbrotherawards.de/2015/technik-hello-barbie.

Thilo Weichert

Systeme biometrischer Identifizierung

Der Siegeszug automatisiert erkannter Fingerabdrücke und Gesichtsbilder






Beim Morphen von zwei Bildern werden an jeweils gleichen Körperstellen positionierte Referenzpunkte automatisiert in beliebig einstellbaren Intervallen zueinander verschoben. Diese Technik, die ursprünglich in der Filmindustrie zur Erzielung von Spezialeffekten eingesetzt wurde, war ein beliebtes Instrument zur missbräuchlichen Verwendung eines Bildes für Ausweisdokumente von zwei Personen. Bilder: Frans Valenta unter Verwendung von AdobeStock-Material

Am 11.12.2020 wurde das **„Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen“** im Bundesgesetzblatt veröffentlicht.[1] Das Gesetz soll die Verfügbarkeit und Zuverlässigkeit staatlicher Identifizierungsmittel durch eine Bereitstellung von authentischen Gesichtsbildern und Fingerabdrücken verbessern. Dem dient die Verhinderung des sog. „Morphing“, also des Verfälschens von Gesichtsbildern zum Zweck der Identitätstäuschung, und die Bereitstellung von automatisiert abgleichbaren Lichtbildern. Dem dient außerdem die verpflichtende Aufnahme der Fingerabdrücke der Zeigefinger in Personaldokumente, insbesondere in Personalausweise, so wie dies zuvor schon für Reisepässe vorgesehen worden ist. Die Regelung des § 5 Abs. 9 S. 1 PAuswG, die zum Fingerabdruck auf dem Ausweis verpflichtet, tritt am 02.08.2021 in Kraft.

Dieses Gesetz ist Anlass, den staatlichen Einsatz biometrischer Identifizierungsverfahren darzustellen und aus Datenschutzsicht zu hinterfragen. **Fingerabdrücke und Gesichtsbilder** sind die Vorreiter biometrischer Identifizierungsmerkmale, mit denen die analoge Welt mit der digitalen Welt verknüpfbar wird und Menschen aus dem Schutz der Anonymität in der Menge herausgezogen werden.

1 Funktionen in der Geschichte

Lange Zeit war in Deutschland die biometrische Identifizierung mit Hilfe technischer Mittel in Verwaltungsverfahren verpönt und wurde als eine Maßnahme angesehen, die der Strafverfolgung zwecks Zuordnung von Tatortspuren und zur **Überführung von Straftätern** vorbehalten ist.

Ein historischer Hintergrund für die deutsche Skepsis bei der Nutzung sol-



Erfassung von Fingerabdrücken zur Strafverfolgung
Bild: iStock.com/TheCrimsonRibbon

cher Identifizierungsmethoden liegt in deren Verwendung im Nationalsozialismus wie auch in der DDR zur Kontrolle und Unterdrückung der Menschen. Dass eine Eignung der Methode für **Kontroll- und Unterdrückungszwecke** heute weiterhin – verstärkt – besteht, zeigt deren Einsatz in autoritären Staaten wie z.B. in China, wo die biometrische Identifizierung als ein zentraler Bestandteil eines totalitären staatlichen Kontrollapparats eingesetzt wird (s.u. 5).

In der **Bundesrepublik Deutschland** wurde es für den identifizierenden Lichtbilderabgleich lange Zeit als ausreichend angesehen, dass ein Beamter das Gesichtsbild aus einem Ausweisdokument oder einer Datenbank mit dem Gesicht des sich Ausweisenden per Augenschein verglich. Von dieser Sichtweise ging man zunächst im Ausländerrecht ab. Die biometrischen Verfahren wurden dann aber bei immer mehr staatlichen Prozessen eingeführt und betreffen immer mehr Menschen und auch solche mit einer deutschen oder einer EU-Staatsangehörigkeit.

Der Prozess der Ausweitung des Einsatzes biometrischer Identifizierung hat verschiedene Gründe. Treibender Faktor ist zweifellos der technische Fortschritt, mit dem die **biometrisch-technische Identifizierung** immer einfacher und zuverlässiger wurde. Die Akzeptanz der Methode wurde zudem dadurch erhöht, dass sie auch von privaten Anbietern genutzt wird, im Arbeits- und insbesondere im Konsumbereich. Der Komfortgewinn durch die Nutzung des Fingerabdrucks oder eines Gesichtsscans bei der betrieblichen Eingangskontrolle, dem Freischalten eines Smartphones oder dem digitalen Bezahlen geht mit einem Gewöhnungseffekt einher, von dem auch der staatliche Einsatz „profitiert".

Hinzu kommen europäische und **weltweite Entwicklungen**: Der globale Personenverkehr ist auf eine eindeutige Identifizierung der mobilen Menschen angewiesen. So legte z.B. die Internationale Zivilluftfahrtorganisation (International Civil Aviation Organization - ICAO) das Lichtbild, den Fingerabdruck und Irismerkmale auf maschinenlesbaren Reisedokumenten als einheitlichen Identifizierungsstandard fest.

Die Notwendigkeit einer **europäischen Harmonisierung und Standardisierung** ergab sich mit der Entwicklung des europäischen Binnenmarkts und der EU-weiten Freizügigkeit für EU-Bürger, was einheitliche Identifizierungsstandards nahelegt. Sog. Drittausländer, also Nicht-EU-Bürger, bei denen sich nicht zwingend auf die staatlich ausgestellten Identitätsdokumente verlassen werden kann, werden über Biometrie identifiziert. Fehlen Identitätsdokumente oder scheinen sie gefälscht, so wie dies bei seit den 90er Jahren verstärkt einreisenden Migranten immer wieder der Fall ist, so sind biometrische Merkmale der einzige Weg für eine sichere Personenzuordnung und Identifizierung.

Werden biometrische Daten zu Zugangs- oder Zutrittszwecken gespeichert, so sind diese ein potenzielles Ziel für Hacker, die diese für **unberechtigte Authentifizierungen** nutzen wollen. Ihre sichere Speicherung ist wesentlich, um Datenmissbrauch zu verhindern. Welche Risiken entstehen können zeigte sich, als 2019 bekannt wurde, dass die Biometriedatenbank „Biostar 2" (Gesichtsbilder und Fingerabdrücke) der südkoreanischen IT-Firma Suprema mit 27,8 Mio. Einträgen über das Internet ohne größeren Aufwand zugänglich war.

2 Gesichtsbilder

Für die rein **analoge Zuordnung** durch einen Menschen finden Gesichtsbilder seit Jahrzehnten selbstverständlichen Einsatz auf Ausweisen und Berechtigungsscheinen im privaten wie im öffentlichen Bereich. So ist es üblich, auf Betriebsausweisen ein Lichtbild aufzunehmen. Die elektronische Gesundheitskarte zum Nachweis der Berechtigung für Leistungen der gesetzlichen Krankenversicherung enthält ein Lichtbild (§ 291 Abs. 2 SGB V). Entsprechendes gilt z.B. für die Fahrerlaubnis für Kraftfahrzeuge – den Führerschein (§ 2 Abs. 1 S. 1 StVG).

Die datenschutzrechtliche **Problematik der Verarbeitung von Gesichtsbildern**, die per Foto- oder Videografie erfasst werden, besteht darin, dass diese jederzeit ohne Beteiligung der Betroffenen aus der Ferne erstellt werden können und dass diese oft mit einer Zuordnungsmöglichkeit zu weiteren Identifizierungsdaten (Name, Adresse, Erreichbarkeitsdaten, sonstige Angaben und Merkmale) im Internet verfügbar sind. Diese Eigenschaft haben Gesichtsbilder mit anderen biometrischen Identifizierungsmethoden gemein, bei denen aus der Ferne bzw. im öffentlichen Raum eine Zuordnung über Mikrofone oder Videokameras möglich ist (Sprechererkennung, Gangzuordnung, s.u. 4). Solche Informationen werden nicht selten von Dritten mit einer eindeutigen Zuordnung öffentlich zugänglich gemacht, etwa im Internet. Oder die Betroffenen veröffentlichen die Informati-

onen selbst, ohne sich dessen bewusst zu sein, dass ihre Veröffentlichung ein Schlüssel dafür ist, sie auch in anderen Kontexten zu identifizieren.

Gesichtsbilder finden sich mit weiteren identifizierenden Angaben und Attributen in großem Umfang allgemein zugänglich im Internet. So hat z.B. die in den USA ansässige Firma Clearview AI aus dem Internet verfügbare Informationen zum Aufbau einer weltweiten Gesichtsbilddatenbank mit angeblich 3 Mrd. Bildern erfasst, die sowohl privaten als auch öffentlichen Stellen zur Nutzung zur Verfügung gestellt wird. Ein vergleichbares Angebot mit 900 Mio. biometrisch analysierten Gesichtern wird als öffentlich nutzbare Suchmaschine von dem polnischen Unternehmen PimEyes betrieben. Facebook praktiziert seit 2010 automatisierte Gesichtserkennung. Diese wurde in Europa 2012 wegen Datenschutzbedenken gestoppt. Seit 2018 ermöglicht das Social-Media-Portal auch in Europa wieder eine Zuordnung von Bildern, wenn die Betroffenen „zustimmen".

Im zentralen **polizeilichen Informationssystem** in Deutschland (INPOL), das vom Bundeskriminalamt (BKA) geführt wird, sind über 5,8 Millionen Lichtbilder von ca. 3,6 Millionen Personen und ca. 3,5 Millionen Personenbeschreibungen aus erkennungsdienstlichen Behandlungen gespeichert (Stand März 2020). Der damit verfolgte Zweck ist die Strafverfolgung und die Gefahrenabwehr (s.u. 9.1). Durch den direkten Zugriff auf INPOL stehen diese Lichtbilder mitsamt Personenbeschreibungen allen deutschen Polizeidienststellen sofort und aktuell zur Verfügung. Mit dem seit 2008 im BKA betriebenen Gesichtserkennungssystem (GES) können einzelne Lichtbilder mit dem Lichtbild-Gesamtbestand automatisiert abgeglichen werden. Das GES trifft eine Vorauswahl aus dem Gesamtbestand. Die Treffer werden anschließend von Lichtbildexperten und -sachverständigen ausgewertet. Im Jahr 2019 wurden bundesweit bei ca. 54.000 Recherchen im GES über 2.100 Personen identifiziert.

Die bisherige zweidimensionale Gesichtserkennung wird nach Weiterentwicklung der Mustererkennungsmethoden durch **dreidimensionale Techniken** ergänzt. Mit einem solchen multibiometrischen System besteht die Möglichkeit, Identifizierungen auch aus partiellen Gesichtsbildaufnahmen mit minderer Bildqualität vorzunehmen.

Gesichtsbilder sind die biometrischen Merkmale, die sich am besten für eine **Öffentlichkeitsfahndung** eignen. Sie können über Fahndungsplakate, über Print- und Digitalmedien und insbesondere auch über das Internet verbreitet werden und ermöglichen es allen Menschen, Zuordnungen vorzunehmen und an die fahndende Stelle zu melden.

Die Qualität der biometrischen Gesichtserfassung wird erhöht, indem bestimmte **Erfassungsstandards** vorgegeben werden und die Erfassung sowie Übermittlung in einer vertrauenswürdigen Umgebung stattfindet. Insofern macht z.B. nun das Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis und ausländerrechtlichen Dokumentenwesen[2] eine Vielzahl von Vorgaben. Es soll damit u.a. das „Morphing" verhindert werden, also die digitale Verfälschung von Gesichtsbildern, die dann von mehr als einer Person genutzt werden und deren Verfälschung im automatisierten Verfahren nicht so leicht erkannt werden kann.

Die Verfügbarkeit staatlich qualitätsgesicherter, automatisiert lesbarer Lichtbilder aus Pässen und Personalausweisen sowie von privaten oder hoheitlichen **Zuordnungsdatenbanken** (z.B. GES des BKA) erhöht das Risiko, dass Menschen anhand ihres Gesichts automatisiert oder konventionell identifiziert werden, ohne dass sie als Betroffene hiervon Kenntnis erlangen. Zugleich erhöht eine solche Verfügbarkeit auch das Risiko, über Tatortbilder in strafrechtliche Ermittlungsverfahren einbezogen zu werden. Diesem Risiko muss mit Hilfe von geeigneten Garantien entgegengewirkt werden (Art. 10 DSRl-JI).

Bisher spielten Gesichtsbildabgleiche außerhalb der Strafverfolgung in Deutschland eine untergeordnete Rolle. Einzig als geeignetes Mittel zur Überführung von Straßenverkehrsverstößen, insbesondere Rotlichtverstößen und Geschwindigkeitsüberschreitungen, wird die Methode durch den analogen Vergleich von Verkehrssünderfotos mit den Bildern in den kommunalen Pass- bzw. Ausweisregistern auf Massenbasis genutzt, wenn der Kfz-Halter bestreitet, der regelverletzende Fahrer zu sein. Die Praxis in China zeigt, dass die Methode zur **Sanktionierung von jeder Art von Regelverstößen** geeignet ist, etwa zur Anprangerung von Rotlichtverstößen (s.u. 5).

In den Jahren 2017/2018 wurde vom Bundesinnenministerium auf dem Bahnhof Berlin-Südkreuz ein Feldversuch zur **automatisierten Gesichtserkennung im öffentlichen Bereich** durchgeführt, der auf starke, auch rechtlich begründete öffentliche Kritik stieß. In Deutschland forderte ein Bündnis von Bürgerrechtsorganisationen „Gesichtserkennung stoppen" ein generelles Verbot automatisierter Gesichtserkennung. In anderen Staaten ist dagegen der automatisierte Gesichtsabgleich für viele Anwendungsfälle schon über das Teststadium hinaus alltägliche Praxis.

3 Fingerabdrücke

Der Fingerabdruck ist die Wiedergabe der **Papillarlinien an der Fingerkuppe** eines Menschen. Diese Linien sind in Bezug auf jeden Menschen einzigartig. Es ist bisher nicht bekannt, dass identische Fingerabdrücke von zwei Menschen gefunden worden sind. Ein Vergleich erfolgt insbesondere über die Poren- und Linienstruktur (Minutien). Zur Extrahierung der Minutien werden diese mit Hilfe von speziellen Algorithmen in eine mathematische Form gebracht.

Anders als Gesichtsbilder sind Fingerabdrücke nicht so leicht zu erlangen. Um auf einfache Weise qualitativ hochwertige Fingerabdrücke zu erhalten, bedarf es einer gewissen Kooperation des Betroffenen. Fingerabdrücke lassen sich aber mit etwas höherem Aufwand auch ohne Beteiligung der Betroffenen erheben, z.B. indem angefasste Objekte (Gläser, Türklinken) auf Fingerabdruckspuren hin ausgewertet werden. Da solche **Spuren fast überall im täglichen Leben** eines Menschen anfallen, ist ein Erlangen von Fingerabdrücken und deren Zuordnung zu einer Person ohne deren Wissen möglich.

Die Erfassung von Fingerabdrücken hat eine lange Tradition in der polizeilichen Praxis zwecks Zuordnung von Tatortspuren. Inzwischen wird das Erfassen und Abgleichen als Identifizierungsme-

thode auch von anderen Behörden und von privaten Stellen genutzt. Anders als die Gesichtserkennung, bei der die Zuordnungsqualität von der Bildperspektive, der Beleuchtung und dem Fehlen von störenden Einflüssen (Haare, Brille, Gesichtsbedeckung) abhängt, kann wegen der Einzigartigkeit der Fingerabdrücke allein mit einem Fingerabdruck in der Regel eine **sichere Zuordnung** vorgenommen werden.

Das BKA führt seit 1951 eine zentrale Fingerabdrucksammlung. 1993 wurde ein **automatisiertes Fingerabdruck-Identifizierungs-System** (AFIS), eingeführt, das auf der Codierung der anatomischen Merkmale (Minutien) basiert (vgl. 8.3, s.u. 9.1). Die Einführung der „Livescan"-Technologie im Jahr 2004 ermöglicht es, die Fingerabdrücke (ebenso wie die der Handflächen) digital aufzunehmen und im zentralen AFIS des BKA zu speichern. Im Rahmen des sog. Fast-ID-Verfahrens können seit 2006 digital aufgenommene Fingerabdrücke ohne Zeitverzug im AFIS recherchiert werden. So sind z.B. im polizeilichen Streifendienst, bei Großveranstaltungen (Fußballspiele, Konzerte etc.) und bei Grenzkontrollen rund um die Uhr innerhalb von wenigen Augenblicken zuverlässige, biometrisch basierte Personenidentifizierungen oder Zuordnungen möglich. Das BKA verarbeitet monatlich ca. 60.000 eingehende digitale Fingerabdruckblätter, die gespeichert, ausgewertet und qualitätsüberprüft werden. Dabei wurden 2019 monatlich rund 19.300 Identifizierungen durch Abgleich von Fingerabdrücken erzielt. Bei Fast-ID ist das Vorgangsaufkommen bisher ähnlich hoch: Hier führt ca. ein Drittel der Anfragen zu einem Treffer im Bestand. Zudem wurden im Jahr 2019 monatlich ca. 30.000 Tatortspuren recherchiert, die im AFIS gespeichert sind, was im Durchschnitt zu ca. 2.200 Treffern führte.

4 Sonstige biometrische Identifizierungsverfahren

Biometrische Identifizierung mit Mitteln der automatisierten Mustererkennung beschränkt sich nicht auf das Gesicht und die Finger. Grundsätzlich eignen sich viele **physiologische und verhaltenstypische Merkmale** zu Identifizierungszwecken, soweit ihnen eine individuelle Eigenheit zukommt. Die Merkmalserfassung kann optisch, akustisch oder mit sonstiger Sensorik, etwa mit chemischen und biotechnischen Verfahren, erfolgen. Beispiele sind die Iris- und die Retinaerkennung, der Abgleich von Handabdrücken, der Scan der Handvenen, die Stimmerkennung (Sprechererkenung), die Zuordnung über den Geruch oder das Mikrobiom, also der bei einem Menschen festgestellten Mikroben. Inzwischen gibt es auch immer mehr Verfahren, mit denen über eine Verhaltensanalyse eine (relativ) sichere individuelle Zuordnung ermöglicht wird, etwa die Analyse der Unterschriftsdynamik, des Tastaturanschlags oder der Mausbewegung am Computer, des Gangs eines Menschen. Auch genetische Daten aus biotechnischen Analysen eignen sich als biometrische Identifizierungsdaten.

5 Staatliche biometrische Identifizierung anderswo

In **Europa** konzentriert sich die staatliche biometrische Identifizierung auf die Bereiche der Sicherheit, der Grenzkontrolle und des Ausländerwesens. Doch bestehen darüber hinausgehende Begehrlichkeiten. So musste z.B. in Schweden ein Schulprojekt mit einem Bußgeld von ca. 18.000 € sanktioniert werden, bei dem mittels Gesichtserkennung die Anwesenheit der Schüler kontrolliert werden sollte. In Italien wurden entsprechende Anwesenheitskontrollversuche bei Schülern mit Fingerabdrücken gemacht. Rechtlich unbeanstandet blieb bisher offenbar das „Loi relative á la protection de l´identité" in Frankreich, das nicht nur die Speicherung von Fingerabdrücken in Personalausweisen und Reisepässen vorsieht, sondern auch deren Speicherung in einem Zentralregister, auf das u.a. die Strafverfolgungsbehörden zugreifen können.

In den **USA** ist automatisierte Gesichtserkennung weit verbreitet und wird schon von privaten Unternehmen für Sicherheitszwecke bei Großveranstaltungen eingesetzt. Strafverfolgungsbehörden nutzen die Gesichtserkennungsdatenbank von Clearview AI. Hiergegen regt sich Widerstand, der u.a. damit begründet wird, dass die Gesichtserkennung vorrangig mit Gesichtern weißer Männer trainiert wurde. Dies führt dazu, dass bei Frauen und nicht-weißen Personen eine sehr viel höhere Fehlerrate vorliegt, was zu einer Diskriminierung der Betroffenen führen kann. Der Widerstand führte dazu, dass Gesichtserkennung in einigen Städten, u.a. San Francisco und Oakland, verboten ist. Amazon untersagte für ein Jahr der US-Polizei die Nutzung seiner Erkennungssoftware „AWS Recognition" wegen der Fehlerrisiken. Microsoft erklärte, mit seinen Produkten Polizeibehörden nicht mehr zu unterstützen zu wollen. Im Januar 2020 startete die US-Regierung mit einer zentralen Speicherung von DNA-Identifizierungsdaten von Flüchtlingen.

In **Brasilien** wurden im Jahr 2019 erstmals Kameras mit Gesichtserkennung eingesetzt, um große Menschenmassen zu kontrollieren. Dies erfolgte z.B. während des Karnevals in Rio mit Hilfe des britischen Facewatch-Systems, wobei die Gesichtsdaten von 1.100 gesuchten Straftätern zum Abgleich hinterlegt wurden. Anwendung findet die Technik auch in Flughäfen. Zum Einsatz kommt dabei auch chinesische Software.

In **Russland** wird in größeren Städten biometrische Gesichtserkennung umfangreich angewendet. 2017 waren in der Hauptstadt Moskau 170.000 Überwachungskameras im Einsatz, die mit der Gesichtserkennung der Firma N-Tech.Lab ausgestattet wurden.

In **Indien** wird im Rahmen des sog. Aadhar-Projektes die größte biometrische Datenbank der Welt aufgebaut. Dabei sollen alle 1,3 Mrd. Inder mit Iris-Scan und Fingerabdruck erfasst werden.

Besonders weit entwickelt ist die biometrische Identifizierung in **China**. Im Wirtschaftsbereich ist Gesichtserkennung etabliert, etwa beim elektronischen Bezahlen über den Messenger-Dienst WeChat. Gesichtserkennung wird genutzt, um Straßenverkehrsverstöße zuzuordnen und die Betroffenen umgehend öffentlich an den Pranger zu stellen. Selbst die Papiernutzung auf Toiletten kann dort per Gesichtsscanning kontrolliert werden. Seit Dezember 2019 bekommt man in China nur noch einen Internet-Anschluss oder eine Mobilfunknummer, wenn zuvor zur

Überprüfung der Identität das Gesicht gescannt wurde. Im November 2019 wurde das National Information Security Standardization Technical Committee gebildet, mit dem Standards für die Identifizierung, zunächst im Bereich der Gesichtserkennung, festgelegt werden. Die Standards sollen alle Bereiche erfassen, auch die regionale und die lokale Verwaltung, die Industrie und die Wirtschaft. Zur erleichterten Kontrolle und Unterdrückung der uigurischen Bevölkerung der westchinesischen Provinz Xinjiang wurde eine umfassende DNA-Bevölkerungsdatenbank etabliert.

6 Internationale Kooperation: Interpol

Die Internationale kriminalpolizeiliche Organisation – Interpol – (englisch International Criminal Police Organization, ICPO) ist ein privatrechtlich organisierter Verein zur Stärkung der Zusammenarbeit nationaler Polizeibehörden. Er wurde 1923 als Internationale kriminalpolizeiliche Kommission in Wien gegründet und hat seinen Sitz in Lyon/Frankreich. Derzeit hat Interpol 194 Mitgliedstaaten. Interpol betreibt **Datenbanken zur forensischen Identifizierung** mit Hilfe von Biometrie. Ziel ist der grenzüberschreitende globale Austausch zwecks Bekämpfung von internationalen Verbrechen, aber auch zwecks Identifizierung von Katastrophenopfern. Alle drei Jahre führt Interpol ein International Fingerprint and Face Symposium durch, das einen weltweiten Austausch über moderne biometrische Identifizierungsmethoden zum Ziel hat.

Die Identifizierung von Katstrophenopfern erfolgt seit 1984 über **Disaster Victim Identification** (DVI), wobei eine Kombination von Abgleichen zu Gesichtsbildern, sonstigen Körpereigenschaften (Tatoos, Implantate, Narben), Finger-, Hand- und Fußabdrücken, Gebissdokumentationen und Genproben genutzt wird. Das deutsche BKA hat hierfür ein unterstützendes DVI Germany Team im Einsatz.

Im Bereich der internationalen Kriminalitätsbekämpfung kommen bei Interpol Verfahren der automatisierten Gesichtserkennung, des Fingerabdruck- und des DNA-Abgleichs zum Einsatz. Das **Interpol Face Recognition System** (IFRIS) wurde 2016 eingeführt und hat mit einer Kombination von automatisierter Suche und analoger Verifizierung seitdem über 1.000 Personen identifiziert. Zum Einsatz kommt bei einigen Mitgliedstaaten zudem eine vollständig automatisierte Treffer-Rückmeldung.

Das von Interpol betriebene **Automatic Fingerprint Identification System** (AFIS) enthält mehr als 220.000 personalisierte Datensätze sowie mehr als 17.000 Tatortspuren. Die Speicherung und der Abgleich erfolgt auf der Grundlage des NIST-Standards (National Institute of Standards and Technology, Version 6.0 von 2020), mit dem JPG-Datensätze einheitlich konvertiert werden können. 2019 konnten so mehr als 1.600 Zuordnungen vorgenommen werden.

2002 wurde bei Interpol eine **DNA-Datenbank** eingerichtet, die mit Stand 2019 von 89 Mitgliedstaaten bestückt wird und 242.000 Datensätze enthält. Gespeichert sind ausschließlich die DNA-Marker in Form eines alphanumerischen Codes; die dazu gehörenden Informationen werden von den Mitgliedsstaaten vorgehalten und auf Einzelanfrage hin übermittelt.

7 Europäische Biometrie-Kooperationen

Folgende **Einrichtungen der EU** sammeln systematisch biometrische Daten für Identifizierungszwecke: Das Schengener Informationssystem (SIS), das Visa-Informationssystem (VIS), Eurodac sowie Europol. 2012 wurde eu-LISA gegründet als Agentur für das Betriebsmanagement der drei großen IT-Systeme für Sicherheit und Migrationskontrolle (SIS, VIS, Eurodac). Für die Speicherung von eingescannten Fingerabdruckbildern verwenden alle in der EU eingesetzten Systeme das gleiche Format. Für die Fingerabdruck-Templates zur Erfassung der Minutien werden hingegen unterschiedliche Formate verwendet.

7.1 Europol

Europäisches Polizeiamt, kurz Europol, ist der Name der EU-Polizeibehörde mit Sitz in Den Haag. Sie soll die Arbeit der nationalen Polizeibehörden Europas im Bereich der grenzüberschreitenden organisierten Kriminalität koordinieren und den Informationsaustausch zwischen den nationalen Polizeibehörden fördern. Seit dem 01.01.2010 ist Europol, das zunächst auf der Grundlage eines völkerrechtlichen Vertrags gegründet wurde, eine Agentur der Europäischen Union. Aktuell gültige Rechtsgrundlage ist die Verordnung (EU) 2016/794 (Europol-VO).[3] Im Anhang II dieser Verordnung werden die personenbezogenen Daten aufgeführt, die gemäß Art. 18 Abs. 2 lit. a Europol-VO erhoben und abgeglichen werden dürfen. Dort sind unter B. lit. c v aufgeführt: *Informationen für die forensische Identifizierung wie Fingerabdrücke, (dem nicht codierenden Teil der DNA entnommene) DNA-Profile, Stimmprofil, Blutgruppe, Gebiss*.

Die Datenspeicherung erfolgt im Europol Informations System (EIS). 2018 waren bei Europol 8.000 Datensätze mit vollständigen zehn **Fingerabdrücken** gespeichert sowie 1.000 einzelne Fingerabdrücke aus Tatortspuren,

Europol soll künftig (ebenso wie die europäische Grenzschutzbehörde Frontex) zur Verfolgung und Prävention terroristischer und anderer schwerer Straftaten einfacheren Zugang zu SIS, Eurodac und VIS erhalten als bisher.

7.2 Schengener Informationssystem

Das Schengener Informationssystem (SIS) wurde 1995 als Kompensations- und Sicherungsmaßnahme nach Abschaffung von Grenzkontrollen zwischen EG-Mitgliedstaaten eingerichtet. Es ist inzwischen die größte hoheitliche Datenbank in Europa und wird als Fahndungsdatenbank von Grenz-, Polizei-, Zollbehörden sowie auch von Geheimdiensten genutzt. Unter der Verantwortung der Europäischen Kommission wurde eine erweiterte Version des SIS (SIS II) entwickelt, in dem seit 2013 (geplant war 2007) auch erstmals **biometrische Daten zu Fahndungszwecken** gespeichert werden. Derzeit sind an dem System 26 EU-Mitgliedstaaten (alle außer Irland und Zypern) sowie Island, Norwegen, Liechtenstein und die Schweiz beteiligt. Zum Stichtag 01.01.2020 waren 90 Mio. Datensätze (Personen und Gegenstände) gespeichert.

Die aktuell gültigen **Rechtsgrundlagen** sind für den ausländerrechtlichen Teil von SIS die Verordnung (EG) Nr. 1987/2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der Zweiten Generation (SIS II-VO)[4] sowie in Bezug auf die Sicherheitsbehörden der Beschluss 2007/533/JI (SIS-II-B).[5] In Art. 1 Abs. 2 SIS-II-VO/SIS-II-B wird der Zweck von SIS II denkbar weit definiert als der Informationsaustausch, *um ein hohes Maß an Sicherheit in dem Raum der Freiheit, der Sicherheit und des Rechts der Europäischen Union, einschließlich der Wahrung der öffentlichen Sicherheit und Ordnung sowie des Schutzes der Sicherheit im Hoheitsgebiet der Mitgliedstaaten, zu gewährleisten*. Eine Ausschreibungskategorie sind Einreise- und Aufenthaltsverweigerungen, wozu Lichtbilder und Fingerabdrücke ausgetauscht werden können (Art. 20 Abs. 2 lit. e, f SIS-II-VO/SIS-II-B). Insofern besteht eine enge Zweckbegrenzung auf die Identitätsbestätigung und (für Fingerabdrücke) die Identitätsfeststellung (Art. 21 Abs. 2, 3 SIS-II-VO, Art. 22 Abs. 2, 3 SIS-II-B). Ein weiterer Zweck besteht in polizeilichen Fahndungsausschreibungen (Art. 20 i.V.m. Art. 26, 32, 34, 36, 38 SIS-II-B: Auslieferungshaft, Vermisste, Durchführung eines Gerichtsverfahrens, Strafverfolgung, Gefahrenabwehr, verdeckte/gezielte Kontrolle). Einen direkten Zugriff auf die Daten haben Grenzkontrollbehörden, der Zoll, die Polizei, Justizbehörden sowie Stellen, die für die Visumerteilung sowie für die Erteilung von Aufenthaltstiteln zuständig sind (Art. 27 SIS-II-VO, Art. 40 SIS-II-B). Auf Daten zur Gefahrenabwehr und Strafverfolgung dürfen auch Europol und Eurojust zugreifen (Art. 41, 42 SIS-II-B). Die SIS-II-Daten können in nationalen Dateien gespeichert werden (Art. 32 SIS-III-VO, Art. 47 SIS-II-B). Erlaubt ist auch die Speicherung von Fingerabdrücken und Lichtbildern sowie sonstiger Identifizierungsdaten zur Missbrauchsverhinderung in Bezug auf Personen, deren Identität missbraucht werden könnte, wenn der Betroffene seine Genehmigung hierzu erteilt (Art. 36 SIS-II-VO/Art. 51 SIS-II-B).

2018 lagen im SIS ca. 121.000 **Fingerabdruckdatensätze** vor, inzwischen sind es über 273.000. 2020 gab es zudem einen Bestand von ca. 63.500 Lichtbildern. Allein die deutschen Behörden konnten 2019 ca. 9.000 Treffer bei biometrischen Suchläufen vorweisen und damit das Vierfache des Vorjahres.

Mit den Verordnungen (EU) 2018/1860, 2018/1861 und 2018/1862[6] erfolgt eine **Erweiterung** des Anwendungsbereichs von SIS II in Bezug auf für die Registrierung von Drittstaatsangehörigen sowie für Bescheinigungen zuständigen Behörden, Verkehrsbehörden oder Stellen, die für Schusswaffen zuständig sind. Angeschlossen wird zudem die europäische Grenzagentur Frontex. Die Zugriffsrechte schon berechtigter Stellen werden ausgeweitet. Zur Speicherung zugelassen werden Licht- und Gesichtsbilder sowie daktyloskopische Daten. Letztere bestehen aus ein bis zehn flachen Fingerabdrücken und *ein bis zehn abgerollten Fingerabdrücken oder bei denen die Erfassung von Fingerabdrücken nicht möglich ist, aus bis zu zwei Handabdrücken*. Die nationale Umsetzung der SIS-Neufassung (SIS 3.0) sollte bis Ende 2021 abgeschlossen sein. Die Federführung für die Umsetzung in Deutschland liegt beim BKA, wobei es drei Teilprojekte (Fachlichkeiten) gibt: Polizei (BKA), Rückkehrentscheidungen (BAMF) und Technik (BKA).

7.3 Eurodac

Mit dem europäischen daktyloskopischen System Eurodac werden **alle zehn Fingerabdrücke von Asylbewerbern und Geflüchteten** EU-weit sowie von Island, Liechtenstein, der Schweiz und Norwegen gespeichert und für Abgleichzwecke bereitgehalten. Das Eurodac-System wurde am 15.01.2003 zunächst in den Mitgliedstaaten der Europäischen Union in Betrieb genommen. Rechtsgrundlage ist heute eine Verordnung der Europäischen Union von 2013, die in den teilnehmenden Mitgliedstaaten unmittelbar gilt (Eurodac-VO).[7] Diese Verordnung löst die ursprüngliche Verordnung von 2000 ab.[8] Um eine länderübergreifende Vergleichsmöglichkeit der Fingerabdrücke zu ermöglichen, werden die Fingerabdrücke in Eurodac nicht als Template, sondern als digitale Bilddaten abgelegt und verglichen.

Die beteiligten Staaten erfassen von den mindestens 14 Jahre (künftig 6 Jahre) alten Asylbewerbern nach Antragstellung oder von ausländischen Personen, die an der Außengrenze oder im grenznahen Raum angetroffen werden, deren jeweilige Fingerabdrücke und übermitteln diese in digitalisierter Form an eine zentrale nationale Stelle (Zentraleinheit), die über die technische Ausstattung zur Speicherung und zum Abgleich verfügt. Erfasst werden die **„Fingerabdruckdaten"**, die in Art. 2 Abs. 1 lit. l Eurodac-VO definiert werden: *Fingerabdruckdaten für sämtliche Finger, mindestens aber für die Zeigefinger, oder sollten diese fehlen, für alle anderen Finger einer Personen oder eine Fingerabdrucksspur*.

Die Datenanlieferung zur Zentraleinheit und die Abfrage von dort erfolgt über eine **„nationale Zugangsstelle"**. In Deutschland ist dies das Bundesamt für Migration und Flüchtlinge (BAMF). Der zentrale Zugang für die deutschen Polizei- und Strafverfolgungsbehörden erfolgt über das BKA. Die Fingerabdruckdaten werden gemeinsam mit einer von dem einspeichernden Mitgliedstaat vergebenen Referenznummer und wenigen Verfahrensdaten an Eurodac übermittelt (Art. 9, 11 Eurodac-VO). Als Ergebnis des elektronischen Abgleichs wird dem anfragenden Mitgliedstaat nur mitgeteilt, ob in der Zentraleinheit bereits übereinstimmende Fingerabdruckdaten vorhanden sind oder nicht (hit/no-hit-System). Im Trefferfall werden zusätzlich die genannten Verfahrensdaten übermittelt. Anhand dieser Angaben kann festgestellt werden, ob die betreffende Person bereits vorher in einem oder mehreren anderen Mitgliedstaaten einen Asylantrag gestellt hat. Die endgültige Identifizierung kann danach von dem anfragenden Mitgliedstaat nach Artikel 15 des Dubliner Übereinkommens in bilateraler Zusammenarbeit mit den betroffenen Mitgliedstaaten vorgenommen werden.

Seit 2015 ist nach Neufassung der Eurodac-VO die Nutzung der Eurodac-Daten auch für den Abgleich zu Zwecken der **Gefahrenabwehr und Strafverfolgung** erlaubt. Hierfür müssen bestimmte Voraussetzungen erfüllt sein, z.B. muss der Datenabgleich im Einzelfall erforderlich sein zur Verhütung, Aufdeckung oder Untersuchung einer terroristischen oder sonstigen schweren

Straftat und ein vorheriger Abgleich mit nationalen Fingerabdruckdateien muss erfolglos geblieben sein.

Inzwischen ist eine **Neufassung der Eurodac-VO** von der EU-Kommission auf den Weg gebracht worden.[9] Darin ist die Herabsetzung des Alters der von einer Fingerabdruckerfassung Betroffenen von 14 auf 6 Jahre vorgesehen. Geplant ist weiterhin eine Änderung in der Speicherpraxis. Geplant ist zudem eine Erfassung des Gesichtsfelds.

7.4 Visa-Informationssystem

Eine Parallele zu Eurodac besteht mit dem europäischen Visa-Informationssystem (VIS), das eine europaweite Koordination der Visa-Erteilung zum Ziel hat und 2011 in Betrieb ging. Rechtliche Grundlage ist die **VIS-Verordnung** (VIS-VO).[10] Gemäß Art. 9 Nr. 6, 6 VIS-VO gibt die Visumbehörde u.a. in das System ein: *5. ein Foto des Antragstellers entsprechend der Verordnung (EG) Nr. 1683/95; 6. Fingerabdrücke des Antragstellers gemäß den maßgeblichen Bestimmungen der Gemeinsamen Konsularischen Instruktion*.

Die Erfassung biometrischer Daten für Visazwecke ist im Visakodex geregelt.[11] Art. 13 Abs. 1 **Visakodex** enthält folgende Regelung: *Die Mitgliedstaaten erfassen im Einklang mit den in der Konvention zum Schutze der Menschenrechte und Grundfreiheiten des Europarates, in der Charta der Grundrechte der Europäischen Union und im VN-Übereinkommen über die Rechte des Kindes verankerten Garantien biometrische Identifikatoren des Antragstellers, nämlich sein Lichtbild und seine zehn Fingerabdrücke*. Die Aufbewahrungsfrist im VIS beträgt nach Art. 23 Abs. 1 VIS-VO höchstens 5 Jahre.

Gemäß Art. 15 Abs. 2 lit. e VIS-VO können die Fingerabdrücke zur **Prüfung der Visumsanträge** abgerufen werden. Art. 18 Abs. 1, Abs. 4 lit. b VIS-VO erlaubt die Abfrage der Fingerabdrücke sowie im Zweifelsfall von Fotos an Außengrenzübergangsstellen *zur Verifizierung der Identität des Visuminhabers und/oder der Echtheit des Visums*. Entsprechendes gilt für die Verifizierung nach Art. 19, 20 VIS-VO innerhalb des Hoheitsgebiets der EU-Mitgliedstaaten, zur Bestimmung der Zuständigkeit für Asylanträge (Art. 21 VIS-VO) sowie zur Prüfung eines Asylantrags (Art. 22 VIS-VO). Eine Löschung erfolgt grds. nach 5 Jahren (Art. 23 VIS-VO).

2018 hat die EU-Kommission eine Überarbeitung der Verordnung sowie damit in Verbindung stehender Verordnungen beschlossen, wodurch der **Zugang von Strafverfolgungsbehörden** zum VIS erleichtert werden soll.[12] Den Zugang deutscher Sicherheitsbehörden zu VIS regelt das VIS-Zugangsgesetz.[13]

2018 waren knapp 48 Mio. Fingerabdruckdatensätze im VIS gespeichert. Künftig soll das VIS mit einer **Gesichtserkennungssoftware** ausgestattet werden. Zudem ist geplant, den automatisierten **Abgleich der Fingerabdrücke** im SIS, im europäischen Einreise-/Ausreisesystem (EES) und im Europäischen Reisegenehmigungssystem (ETIAS) „mit einem einzigen Klick" zu ermöglichen (s.u. 7.6).

7.5 Prümer Vertrag

Der **Prümer Vertrag** ist ein zwischenstaatliches Abkommen zwischen derzeit 13 Mitgliedstaaten der EU, das die grenzüberschreitende Zusammenarbeit und insbesondere den Informationsaustausch zwischen den Vertragsparteien zum Zweck der Verhinderung und Verfolgung von Straftaten und der illegalen Migration verbessern soll. Das Abkommen mit der amtlichen Bezeichnung „Vertrag über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration" wurde am 27.05.2005 im rheinland-pfälzischen Prüm geschlossen. Signatarstaaten sind Belgien, Deutschland, Spanien, Frankreich, Luxemburg, die Niederlande und Österreich. Dem Abkommen beigetreten sind bisher Bulgarien, Estland, Finnland, Rumänien, die Slowakei und Ungarn. Die anderen EU-Mitgliedstaaten können dem Vertrag beitreten; sie sind dazu jedoch nicht verpflichtet. Der Vertrag von Prüm ist kein EU-Abkommen.

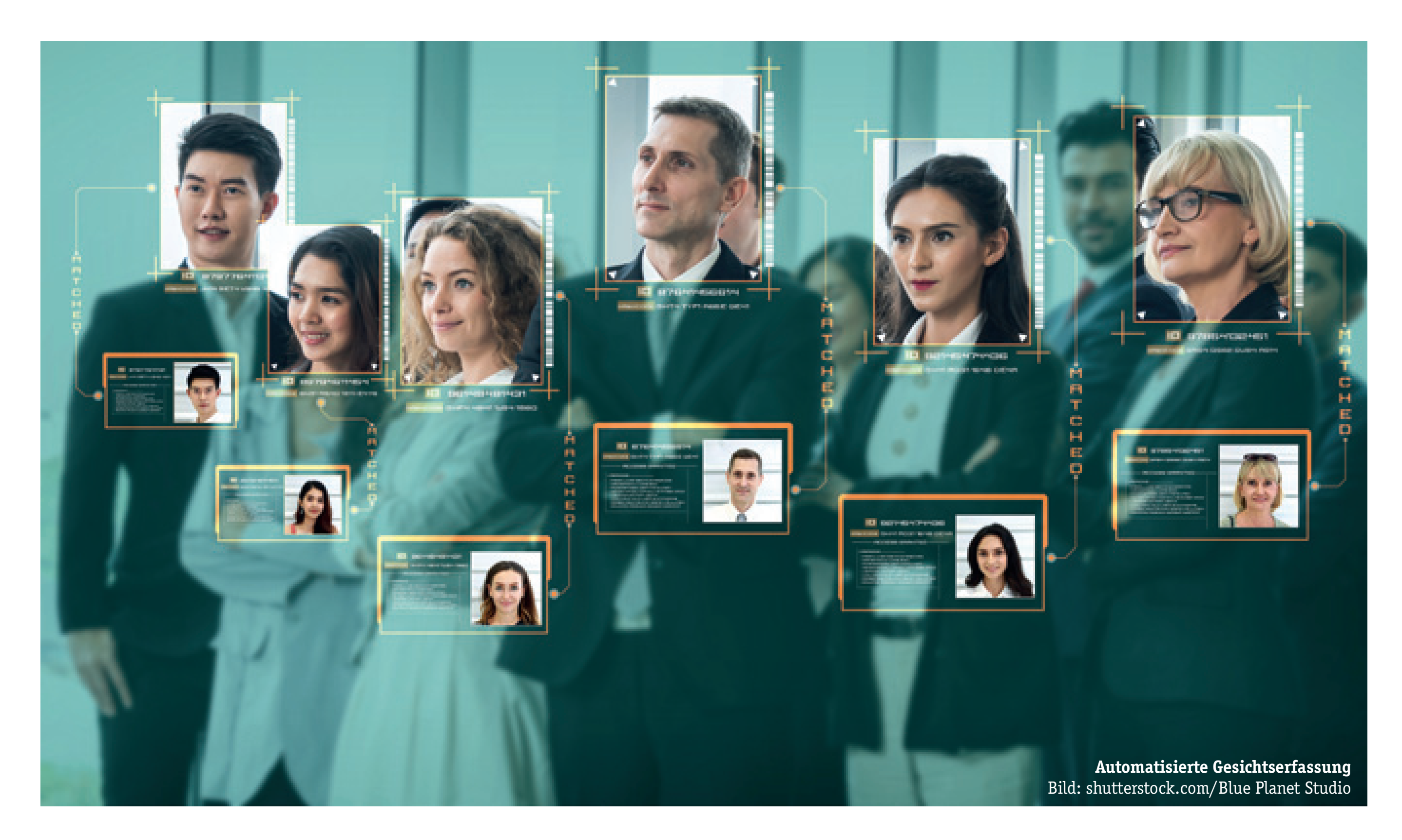
Der Prümer Vertrag sieht vor, dass Polizei- und Strafverfolgungsbehörden direkt auf bestimmte Datenbanken zugreifen können, die von den Behörden der anderen Vertragsstaaten geführt werden. Die Zugriffsberechtigung erstreckt sich u.a. auch auf **elektronisch gespeicherte Fingerabdrücke**, in Deutschland also auf die in AFIS gespeicherten Daten. Seit Februar 2008 tauschen Deutschland, Luxemburg und Österreich daneben als weltweit erste Staaten im automatisierten Verfahren auch Fingerabdruckdaten aus. Weiterhin erlaubt der Vertrag zu Zwecken einer eindeutigen biometrischen Identifizierung den Zugriff auf DNA-Analyse-Dateien, in Deutschland also auf die DNA-Datenbank des Bundeskriminalamts (BKA).

Derzeit errichten die Firmen IDEMIA und Sopra Steria für die EU ein biometrischen Erkennungssystem, wozu Fingerabdrücke und Gesichtsbilder aus fünf nationalen Datenbanken in einer Datei zusammengeführt werden und damit eine **europaweite Interoperabilität biometrischer Datenbanken** erreicht werden soll.

7.6 Einreise-/Ausreisesystem

Die EU realisiert zudem ein Ein-/Ausreisesystem (EES), womit sämtliche Ein- und Ausreisen von Drittstaatsangehörigen an den Schengener Außengrenzen erfasst werden – und zwar nicht beschränkt auf die visumspflichtigen Drittausländer, deren Visa bereits im VIS gespeichert sind. Beim Grenzübertritt werden dann die in den Reisedokumenten enthaltenen **Gesichtsbilder und Fingerabdrücke ausgelesen** und zusammen mit den Personalien sowie den Angaben über frühere Aufenthalte für fünf Jahre gespeichert.

Mit dem Ein-/Ausreisesystem gekoppelt werden soll zudem das **Reiseinformations- und -genehmigungssystem** (ETIAS). Dieses soll eine „Vorabinformation" über die geplante Einreise visumsbefreiter Drittstaatsangehöriger möglich machen, die ihre Reise neu auf einem Internetformular ankündigen müssen. Vorab würden die entsprechenden Daten von den zuständigen Grenzbehörden mit nationalen und internationalen Informationssystemen abgeglichen. Europol soll hierfür eine „Watchlist" erstellen, um die Einreise von unerwünschten Ausländern zu verhindern.



Automatisierte Gesichtserfassung
Bild: shutterstock.com/Blue Planet Studio

8 Erfassung von Ausländern nach deutschem Recht

Parallel zur biometrischen Identifizierung nach europaweiten Vorgaben erfolgt der Einsatz der Methode auf der Grundlage des deutschen Ausländerrechts. Dieser Einsatz ist dadurch gekennzeichnet, dass dabei **keine strengen Erforderlichkeits- und Zweckprüfungen** stattfinden.

8.1 Ausländerzentralregister

Seit 1953 besteht in der Bundesrepublik Deutschland ein Ausländerzentralregister (AZR), das seit 1967 automatisiert geführt wird. Darin erfasst sind **alle Nichtdeutschen**, die sich nicht nur vorübergehend in der Bundesrepublik aufhalten. Das ursprünglich von Bundesverwaltungsamt (BVA) betriebene AZR steht seit 2004 in der rechtlichen Verantwortung des Bundesamtes für Migration und Flüchtlinge (BAMF). Die Identifizierung der Betroffenen erfolgte ursprünglich auf der Grundlage der von diesen zur Verfügung gestellten Dokumente. Erfasst wurden die sog. Grundpersonalien (Namen, Schreibweisen der Namen, Geburtsangaben, Geschlecht, Staatsangehörigkeit) sowie „weitere Personalien" (u.a. abweichende Schreibweisen, andere, frühere und Aliasnamen, Familienstand, Angaben zum Ausweispapier).[14] Biometrische Daten wurden zunächst nicht im AZR gespeichert.

Das Lichtbild wird seit 2002 in der Visa-Datei des AZR, in der Visaanträge vermerkt werden, gespeichert (§ 29 Abs. 1 Nr. 4 AZRG). In den allgemeinen Datenbestand des AZR wurde das Lichtbild mit Gesetz vom 19.08.2007 in § 3 Abs. 1 Nr. 5a AZRG 2007 aufgenommen.[15] Damit soll die Identitätsfeststellung bei abfragenden Stellen, die einen direkten Kontakt zum Ausländer haben, erleichtert werden. Voraussetzung für die Erteilung eines Aufenthaltstitels ist die eindeutige Identifizierung (§ 5 Abs. 1 Nr. 1a AufenthG). Das Lichtbild wurde vom Gesetzgeber als ein zuverlässiges, weil wenig veränderliches Datum eingestuft.

Die Lichtbildangaben von **EU-Bürgern**, die innerhalb der EU Freizügigkeit genießen, wurden mit Gesetz vom 27.12.2012 wieder aus dem AZR-Datenbestand herausgenommen (§ 3 Abs. 4 AZRG).[16] Hintergrund dieser Änderung war, dass der Europäische Gerichtshof 2008 festgestellt hatte, dass diese und weitere Speicherungen sowie insbesondere Datennutzungen für Zwecke der Kriminalitätsbekämpfung in Bezug auf EU-Bürger zu einer Diskriminierung im Vergleich zu deutschen Staatsangehörigen führten.[17]

Mit Gesetz vom 02.02.2016[18] wurde die Speicherung von **Fingerabdruckdaten** im AZR eingeführt. Diese werden aber nicht von allen Ausländern erfasst, sondern nur von Flüchtlingen und unzulässig aufhältigen Ausländern: Betroffen ist nach § 3 Abs. 2 Nr. 1 AZRG ein Ausländer, der *1. ein Asylgesuch geäußert hat, 2. unerlaubt eingereist ist oder 3. sich unerlaubt im Geltungsbereich dieses Gesetzes aufhält* (§ 2 Abs. 1a AZRG). Derart erfasst werden zudem Ausländer, *die einen Asylantrag gestellt haben oder über deren Übernahme nach den Rechtsvorschriften der Europäischen Gemeinschaft oder eines völkerrechtlichen Vertrages zur Durchführung eines Asylverfahrens entschieden ist* (§ 2 Abs. 2 Nr. 1 AZRG). Im AZR werden zusätzlich zu den Fingerabdruckdaten die dazu gehörigen Referenznummern gespeichert (§ 3 Abs. 2 Nr. 1 AZRG). Mit diesen sog. D-Nummern soll eine Zuordnung der Daten im AZR zu den Beständen im polizeilichen INPOL-System vorgenommen werden können.

2019 wurde mit § 3 Abs. 3a AZRG der Kreis der Personen, von denen im AZR

Fingerabdrücke (und Referenzdaten) gespeichert werden, erweitert um Ausländer, *für oder gegen die aufenthaltsrechtliche Entscheidungen getroffen worden sind oder die Antrag auf einen Aufenthaltstitel oder passrechtliche Maßnahme gestellt haben, ausgenommen Entscheidungen und Anträge im Visaverfahren* (§ 2 Abs. 2 Nr. 3 AZRG). Es handelt sich um Ausländer, die aus dem Ausland aufgenommen werden sollen (Resettlement-, Relocation-, sonstige humanitäre Aufnahmeverfahren und Dublin-Übernahmeersuchen). Die **zusätzliche Speicherung** wurde wieder mit der besseren Identifizierbarkeit, diesmal im Rahmen des Abgleichverfahrens, begründet.

Ein Hauptzweck der Einführung einer Spezialregelung für Flüchtlinge im AZRG bestand darin, einen gesetzlichen Rahmen für einen frühzeitigen Informationsaustausch über diese zwischen verschiedenen öffentlichen Stellen nach einer **qualifizierten Identitätsprüfung** vornehmen zu können. Hierfür nutzt das BAMF weitere neue automatisierte Instrumente. Dazu gehört ein Transliterationsassistent (TraLiTa), mit dem bei arabischsprachigen Antragstellern arabische Schriftzeichen einheitlich in lateinische Buchstaben übertragen werden, ein automatisiertes sprachbiometrisches Analysesystem, mit dem Sprachproben einer Dialektanalyse unterworfen werden, um Herkunftsregionen festzustellen, und die Auswertung von Handydaten, um Rückschlüsse auf Kontakte und Fluchtwege ziehen zu können.

8.2 Aufenthalts- und Asylgesetz

Vor der zentralen AZR-Speicherung fanden sich biometrische Daten schon in den Akten und Dateien der **Ausländer- und Asylbehörden**. § 49 Abs. 1 AufenthG hat heute folgenden Wortlaut:

Die mit dem Vollzug dieses Gesetzes betrauten Behörden dürfen unter den Voraussetzungen des § 48 Abs. 1 die auf dem elektronischen Speicher- und Verarbeitungsmedium eines Dokuments nach § 48 Abs. 1 Nr. 1 und 2 gespeicherten biometrischen und sonstigen Daten auslesen, die benötigten biometrischen Daten beim Inhaber des Dokuments erheben und die biometrischen Daten miteinander vergleichen. Darüber hinaus sind auch alle anderen Behörden, an die Daten aus dem Ausländerzentralregister nach den §§ 15 bis 20 des AZR-Gesetzes übermittelt werden, und die Meldebehörden befugt, Maßnahmen nach Satz 1 zu treffen, soweit sie die Echtheit des Dokuments oder die Identität des Inhabers überprüfen dürfen. Biometrische Daten nach Satz 1 sind nur die Fingerabdrücke und das Lichtbild.

§ 49 Abs. 1 AufenthG nimmt Bezug auf § 48 Abs. 1 Nr. 1 u. 2 AufenthG, der die **ausweisrechtlichen Pflichten von Ausländern** regelt:
Ein Ausländer *ist verpflichtet,*
1. seinen Pass, seinen Passersatz oder seinen Ausweisersatz und
2. seinen Aufenthaltstitel oder eine Bescheinigung über die Aussetzung der Abschiebung auf Verlangen den mit dem Vollzug des Ausländerrechts betrauten Behörden vorzulegen, auszuhändigen und vorübergehend zu überlassen, soweit dies zur Durchführung oder Sicherung von Maßnahmen nach diesem Gesetz erforderlich ist.

§ 49 Abs. 7 AufenthG erlaubt ein weiteres biometrisches Verfahren zur Bestimmung des Herkunftsstaates oder der Herkunftsregion des Ausländers: Das **gesprochene Wort** des Ausländers darf auf Ton- oder Datenträgern aufgezeichnet werden, wenn der Ausländer vorher darüber in Kenntnis gesetzt wurde.

Mit dem Terrorismusbekämpfungsgesetz[19] wurde 2002 das damalige Ausländergesetz dahingehend geändert, dass in die Dokumente über den jeweiligen **Aufenthaltstitel** biometrische Merkmale aufgenommen wurden. Gemäß § 48 Abs. 2 AufenthG *genügt ein Ausländer, der einen Pass oder Passersatz weder besitzt noch in zumutbarer Weise erlangen kann, … der Ausweispflicht mit der Bescheinigung über einen Aufenthaltstitel oder die Aussetzung der Abschiebung, wenn sie mit den Angaben zur Person und einem Lichtbild versehen und als Ausweisersatz bezeichnet ist*. So ist über diesen „Ausweisersatz" gewährleistet, dass mit dem Lichtbild eine biometrische Identifizierung erfolgen kann.

Gemäß § 49 Abs. 6, 6a AufenthG sind die typischen Verfahren zur **Feststellung der Identität** *das Aufnehmen von Lichtbildern und das Abnehmen von Fingerabdrücken*.

Bisher war die Durchführung dieser Maßnahmen auf Ausländer ab dem 14. Lebensjahr beschränkt (§ 49 Abs. 6 S. 2 AufenhG, ebenso § 16 Abs. 1 S. 2 AsylG). Am 01.04.2021 tritt eine Neuregelung in Kraft, wonach die Erfassung von Fingerabdrücken schon **ab dem 6. Lebensjahr** zulässig ist.[20] Hintergrund dieser Ausweitung ist, dass auf EU-Ebene eine Änderung der Eurodac-VO und der Verordnung über das Visa-Informationssystems anstand, die eine Erfassung der Fingerabdrücke schon ab dem 6. Lebensjahr vorsieht.[21] Es wird damit in Kauf genommen, dass wegen des Wachsens der Kinder Qualitätsdefizite bei den Abdrücken auftreten, da diese noch Wachstumsprozessen und Änderungen ausgesetzt sind.

Das **Verfahren der ausländerrechtlichen Identitätsprüfung** ist in § 89 AufenthG geregelt:
(1) Das Bundeskriminalamt leistet Amtshilfe bei der Auswertung der nach § 49 von den mit der Ausführung dieses Gesetzes betrauten Behörden erhobenen und nach § 73 übermittelten Daten. Es darf hierfür auch von ihm zur Erfüllung seiner Aufgaben gespeicherte erkennungsdienstliche Daten verwenden. Die nach § 49 Abs. 3 bis 5 sowie 8 und 9 erhobenen Daten werden getrennt von anderen erkennungsdienstlichen Daten gespeichert. Die Daten nach § 49 Abs. 7 werden bei der aufzeichnenden Behörde gespeichert.
(1a) Im Rahmen seiner Amtshilfe nach Absatz 1 Satz 1 darf das Bundeskriminalamt die erkennungsdienstlichen Daten nach Absatz 1 Satz 1 zum Zwecke der Identitätsfeststellung auch an die für die Überprüfung der Identität von Personen zuständigen öffentlichen Stellen von Drittstaaten mit Ausnahme des Herkunftsstaates der betroffenen Person sowie von Drittstaaten, in denen die betroffene Person eine Verfolgung oder einen ernsthaften Schaden zu befürchten hat, übermitteln. Die Verantwortung für die Zulässigkeit der Übermittlung trägt das Bundeskriminalamt. Das Bundeskriminalamt hat die Übermittlung und ihren Anlass aufzuzeichnen. Die empfangende Stelle personenbezogener Daten ist darauf hinzuweisen, dass sie nur zu dem Zweck verarbeitet werden dürfen, zu dem sie übermittelt worden sind. Ferner ist ihr

der beim Bundeskriminalamt vorgesehene Löschungszeitpunkt mitzuteilen. Die Übermittlung unterbleibt, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass
1. unter Berücksichtigung der Art der Daten und ihrer Erhebung die schutzwürdigen Interessen der betroffenen Person, insbesondere ihr Interesse, Schutz vor Verfolgung zu erhalten, das Allgemeininteresse an der Übermittlung überwiegen oder
2. die Übermittlung der Daten zu den Grundrechten, dem Abkommen vom 28. Juli 1951 über die Rechtsstellung der Flüchtlinge sowie der Konvention zum Schutz der Menschenrechte und Grundfreiheiten in Widerspruch stünde, insbesondere dadurch, dass durch die Verarbeitung der übermittelten Daten im Empfängerstaat Verletzungen von elementaren rechtsstaatlichen Grundsätzen oder Menschenrechtsverletzungen drohen.
(2) Die Verarbeitung der nach § 49 Abs. 3 bis 5 oder Abs.7 bis 9 erhobenen Daten ist auch zulässig zur Feststellung der Identität oder der Zuordnung von Beweismitteln im Rahmen der Strafverfolgung oder zur polizeilichen Gefahrenabwehr. Sie dürfen, soweit und solange es erforderlich ist, den für diese Maßnahmen zuständigen Behörden übermittelt oder bereitgestellt werden.
(3) Die nach § 49 Abs. 1 erhobenen Daten sind von allen Behörden unmittelbar nach Beendigung der Prüfung der Echtheit des Dokuments oder der Identität des Inhabers zu löschen. Die nach § 49 Abs. 3 bis 5, 7, 8 oder 9 erhobenen Daten sind von allen Behörden, die sie speichern, zu löschen, wenn
1. dem Ausländer ein gültiger Pass oder Passersatz ausgestellt und von der Ausländerbehörde ein Aufenthaltstitel erteilt worden ist,
2. seit der letzten Ausreise, der versuchten unerlaubten Einreise oder der Beendigung des unerlaubten Aufenthalts zehn Jahre vergangen sind,
3. in den Fällen des § 49 Abs. 5 Nr. 3 und 4 seit der Zurückweisung oder Zurückschiebung drei Jahre vergangen sind oder
4. im Falle des § 49 Abs. 5 Nr. 5 seit der Beantragung des Visums sowie im Falle des § 49 Abs. 7 seit der Sprachaufzeichnung zehn Jahre vergangen sind.
Die Löschung ist zu protokollieren.
(4) Absatz 3 gilt nicht, soweit und solange die Daten im Rahmen eines Strafverfahrens oder zur Abwehr einer Gefahr für die öffentliche Sicherheit oder Ordnung benötigt werden.

Die Funktion der Identifizierungsdaten von Ausländern hat sich mit der Zeit ausgeweitet. Der Grundsatz ist, dass die erkennungsdienstlichen Unterlagen zu vernichten sind, nachdem *dem Ausländer ein gültiger Pass oder Passersatz ausgestellt und von der Ausländerbehörde eine Aufenthaltsgenehmigung erteilt worden ist* (so § 78 Abs. 4 S. 1 Nr. 1 AuslG, vgl. jetzt § 89 Abs. 3 S. 2 Nr. 1 AufenthG). Nach § 89 AufenthG kommt den ED-Unterlagen nun der zusätzliche Zweck der Datenbevorratung für eine **künftige Identifizierung in Zweifelsfällen** zu: Der Ausländer könnte später unter einer anderen Identität versuchen, einen Aufenthaltstitel zu erlangen.

Während im Aufenthaltsgesetz die biometrische Identifizierung davon abhängt, dass diese erforderlich ist, verpflichtet § 16 Abs. 1, 2 AsylG **in jedem Fall eines Asylgesuchs** zu dieser Maßnahme:
(1) Die Identität eines Ausländers, der um Asyl nachsucht, ist durch erkennungsdienstliche Maßnahmen zu sichern. Nach Satz 1 dürfen nur Lichtbilder und Abdrucke aller zehn Finger aufgenommen werden; soweit ein Ausländer noch nicht das 14. Lebensjahr vollendet hat, dürfen nach Satz 1 nur Lichtbilder aufgenommen werden. Zur Bestimmung des Herkunftsstaates oder der Herkunftsregion des Ausländers kann das gesprochene Wort außerhalb der förmlichen Anhörung des Ausländers auf Ton- oder Datenträger aufgezeichnet werden. Diese Erhebung darf nur erfolgen, wenn der Ausländer vorher darüber in Kenntnis gesetzt wurde. Die Sprachaufzeichnungen werden beim Bundesamt gespeichert.
(1a) Zur Prüfung der Echtheit des Dokumentes oder der Identität des Ausländers dürfen die auf dem elektronischen Speichermedium eines Passes, anerkannten Passersatzes oder sonstigen Identitätspapiers gespeicherten biometrischen und sonstigen Daten ausgelesen, die benötigten biometrischen Daten erhoben und die biometrischen Daten miteinander verglichen werden. Biometrische Daten nach Satz 1 sind nur die Fingerabdrücke, das Lichtbild und die Irisbilder.

8.3 AFIS beim BKA

Die zentrale **Fingerabdrucksammlung des Bundeskriminalamtes** (BKA) wurde seit dessen Gründung im Jahr 1951 kontinuierlich ausgebaut. Im Jahr 1976 nahm das erste halbautomatische Datenverarbeitungssystem zur Auswertung von Fingerabdrücken den Wirkbetrieb auf. Ein verbessertes, automatisiertes Fingerabdruck-Identifizierungs-System (AFIS) wurde im Jahr 1993 eingeführt. Es basiert auf der Codierung der anatomischen Merkmale (Minutien), die im Finger- und Handflächenabdruck abgebildet sind. Das System kann die Minutien automatisch erkennen und mit dem Code der abgespeicherten Fingerabdrücke und -spuren vergleichen. Seit 2003 werden im AFIS auch Handflächenabdrücke systematisch ausgewertet.

BKA-Präsident Holger Münch kündigte 2017 an, dass Deutschland als erstes europäisches Land seine Fingerabdruck-Datenbank AFIS an das Schengener Informationssystem SIS II anschließt (s.o. 7.2). Während dort bisher nur nach Personennamen gefahndet werden konnte, ist dies nun auch mittels Fingerabdruck möglich. Deutschland arbeitet unter der Federführung Frankreichs an einem neuen Abfragesystem, das den Abruf von Fingerabdrücken und weiteren Biometrie-Daten nach dem Prümer Vertrag **über ganz Europa hinweg** vereinfacht (s.o. 7.5).

Bei AFIS wird unterschieden zwischen einem Bestand AFIS-P, den das BKA auf Grund seiner originären Zuständigkeit im Bereich der Gefahrenabwehr und der Strafverfolgung speichert (s.u. 9.1), sowie dem sich auf Ausländer beziehenden Bestand AFIS-A. Insofern ist das BKA gemäß § 1 Abs. 3 AZRG in **Amtshilfe** tätig bei der Verarbeitung der Daten nach § 16 Abs. 1 S. 1 AsylG und § 49 AufenthG. In § 1 Abs. 3 S. 2 AZRG heißt es: *Sie werden dort getrennt von anderen erkennungsdienstlichen Daten gespeichert*. Entsprechende Amtshilfevorschriften gibt es in § 16 Abs. 3, 3a, 4 AsylG und § 89 Abs. 1 AufenthG. Die Amtshilfeverpflichtung des BKA besteht im Asylverfahren bereits seit 1993 und wurde 2007 auf die Daten nach § 49 AufenthG erweitert.

Die Fingerabdrücke werden in der **Fingerabdruckdatei AFIS-A** mit ei-

ner recherchierbaren Referenznummer gespeichert, die auf die Identitätsprüfungen nach § 16 AsylG durch Aufnahmeeinrichtungen, Mobile Teams und Außenstellen des BAMF verweisen. Seit dem 25.10.2017 besteht insofern eine sog. AsylOnline-Schnittstelle bzw. zur Personengruppe nach § 49 AufenthG eine sog. AZR-Erstregistrierungsschnittstelle (AZR-ER-SST).

Die Amtshilferegelungen erklären sich traditionell damit, dass die Auswertung von ED-Unterlagen und insbesondere von Fingerabdrücken für die Kriminalitätsbekämpfung entwickelt worden ist und insofern das BKA die nötige Expertise vorweisen konnte. Inzwischen ist die Technik so weiterentwickelt, dass es anderen Stellen problemlos möglich wäre, diese Aufgaben selbst wahrzunehmen. Durch die weiterhin erfolgende Einschaltung ist es dem BKA als Polizeibehörde leicht, die bei sich aus „Amtshilfegründen" gespeicherten Daten **auch für eigene Zwecke** zu nutzen.

Der Begriff der Amtshilfe ist dem Datenschutzrecht fremd. Insofern wird nur zwischen Verantwortlichem (Art. 4 Nr. 7, 24, 26 DSGVO) und Auftragsverarbeiter (Art. 4 Nr. 8, 28 DSGVO) unterschieden. Die Verarbeitung durch das BKA erfolgt vorrangig als **Auftragsverarbeitung**; Verantwortlicher ist i.d.R. das BAMF als für das AZR und für die Verarbeitung im Asylverfahren verantwortliche Stelle. Verantwortlich kann bei einer Erhebung nach § 48 AufenthG aber auch jede tätig werdende Ausländerbehörde werden.

Die vorgesehene **Trennung** der ausländerrechtlichen AFIS-Daten von anderen erkennungsdienstlichen Daten hat keine erkennbare räumliche, organisatorische oder funktionale Bedeutung. Es erfolgt zwischen AFIS-A (Ausländer) und AFIS-P (Polizei) lediglich eine spezifische technische Markierung. Die gesetzlich vorgesehene Trennung gewährleistet nicht, dass das BKA für die Daten keine Nutzungsbefugnis für die eigenen Zwecke der Gefahrenabwehr und der Strafverfolgung hat. Diese Eigennutzung ist ausdrücklich gesetzlich erlaubt (§ 15 Abs. 1 S. 1 Nr. 5 AZRG, § 89 Abs. 2 AufenthG, § 16 Abs. 5 AsylG). Die Trennung ist damit keine von der DSGVO geforderte wirksame Garantie bzw. technisch-organisatorische Sicherungsmaßnahme.

9 Sicherheitsbehörden

Fingerabdrücke und Lichtbilder sind **klassische Informationsgrundlagen** für Sicherheitsbehörden. In jüngerer Zeit werden weitere biometrische Verfahren zur Identifizierung von Personen, seien es Täter, Opfer oder Dritte, eingesetzt.

9.1 Strafverfolgung und Gefahrenabwehr

Der primäre Zweck biometrischer Identifizierung durch Sicherheitsbehörden ist die Strafverfolgung. Damit werden tatrelevante Spuren Personen zugeordnet, um Beteiligte, Zeugen und insbesondere Täter zu identifizieren. Die Methode wird **„Erkennungsdienst"** (ED) bezeichnet. Die gesetzliche Grundlage hierfür findet sich in § 81b StPO mit folgendem Wortlaut:

Soweit es für die Zwecke der Durchführung des Strafverfahrens oder für die Zwecke des Erkennungsdienstes notwendig ist, dürfen Lichtbilder und Fingerabdrücke des Beschuldigten auch gegen seinen Willen aufgenommen und Messungen und ähnliche Maßnahmen an ihm vorgenommen werden.

Eine ED-Untersuchung von anderen Personen als Beschuldigten ist unter bestimmten Voraussetzungen nach § 81c StPO möglich. Erkennungsdienstliche (ED-) Maßnahmen sind auch nach § 24 Abs. 3 BPolG, nach § 20e BKAG oder gemäß **polizeirechtlichen Regelungen** der Bundesländer zulässig.

Die Fingerabdrücke von Beschuldigten eines Ermittlungsverfahrens werden bei Vorliegen der rechtlichen Voraussetzungen dem BKA zwecks Speicherung im zentralen **Fingerabdruckidentifizierungssystem** (AFIS-P) übermittelt. Eine weitere Übermittlung durch das BKA erfolgt an Eurodac, wenn Art. 14 i.V.m. Art. 17 Eurodac-VO (illegaler Grenzübertritt/illegaler Aufenthalt) zum Tragen kommt und die erkennungsdienstlich behandelte Person älter als 14 Jahre ist, oder zum Zwecke der Gefahrenabwehr und Strafverfolgung (bei Vorliegen terroristischer oder sonstiger schwerer Straftaten), und zusätzlich wenn vorher die Abfragen aller anderen nationalen und internationalen Dateien zu keiner Identifizierung geführt haben.

Die Identifizierung mit dem „genetischen Fingerabdruck" fand in den 90er Jahren Eingang ins Strafverfahren und wurde seitdem immer mehr ausgeweitet (§§ 81e-81 h StPO). Beim BKA wird eine DNA-Datenbank geführt. Mit dem bayerischen Polizeiaufgabengesetz von 2018 schaffte die **DNA-Analyse** zur Feststellung biologischer Merkmale (Farbe von Haar, Haut und Augen), des Alters sowie der biogeografischen Herkunft ihre erste gesetzliche Anerkennung im Bereich der Gefahrenabwehr. 2019 wurde die Methode zur Feststellung von Merkmalen und Alter auch in § 81e Abs. 2 der Strafprozessordnung zu strafrechtlichen Ermittlungen zugelassen.

Im **Strafvollzugsrecht** ist ebenso die Vornahme von ED-Maßnahmen vorgesehen und umfasst u.a. Finger- und Handflächenabdrücke, Lichtbilder sowie weitere äußere Merkmale und Messungen.

9.2 Geheimdienste

Die deutschen Geheimdienste, der Auslandsdienst BND (Bundesnachrichtendienst), der MAD (Militärischer Abschirmdienst), das Bundesamt für Verfassungsschutz (BfV) sowie die Landesbehörden für Verfassungsschutz betreiben das zunächst als analoge Datensammlung geführte und später digitalisierte **Nachrichtendienstliche Informationssystem** (NADIS). Es handelt sich um eine Hinweisdatei, die der Identifizierung einer Person, Organisation oder eines Sachverhaltes und dem Auffinden von Aktenfundstellen dient. Eine Speicherung im NADIS darf nur aufgrund der in den Verfassungsschutzgesetzen definierten gesetzlichen Regelungen erfolgen. Diese Regelungen enthalten keine speziellen Aussagen zur Speicherung biometrischer Identifizierungsdaten. Dies schließt aber die Personenidentifizierung mit derartigen Merkmalen nicht aus. Bei der nachrichtendienstlichen Tätigkeit spielt die biometrische Identifikation wohl eine geringere Rolle als bei der Gefahrenabwehr und Strafverfolgung durch die Polizei.

Die Nachrichtendienste können sich die **Sammlung von Identifizierungsdaten** anderer Behörden nutzbar machen. Dies gilt für Lichtbilder und

Fingerabdrücke des Ausländerzentralregisters, die automatisiert abgerufen werden dürfen (§ 20, 22 Abs. 1 S. 1 Nr. 9 AZRG). Sie haben ebenso den automatisierten Zugriff auf die Lichtbilder der Pass- und das Personalausweisregister der Kommunen (§ 22a Abs. 2 S. 4 PassG u. § 25 Abs. 2 S. 4 PAuswG). Direkten Zugriff nehmen können die Nachrichtendienste auch auf gemeinsame mit der Polizei geführten Datenbanken wie z.B. seit 2007 die Anti-Terror-Datei (ATD) oder seit 2012 die Rechtsextremismusdatei (RED). Gespeichert sind dort zu Personen aus den Bereichen Terrorismus oder Gewaltextremismus keine Fingerabdrücke, wohl aber biometrisch „besondere körperliche Merkmale“, Lichtbilder und Angaben zu Identitätspapieren (§§ 2, 3 Abs. 1 Nr. 1a ATDG, §§ 2, 3 Abs. 1 Nr. 1a RED-G). Gemäß § 17 BKAG kann das Bundeskriminalamt für die Dauer einer befristeten projektbezogenen Zusammenarbeit mit den Verfassungsschutzbehörden des Bundes und der Länder, dem MAD und dem BND (ebenso wie mit den Polizeibehörden des Bundes und der Länder und dem Zollkriminalamt) unter bestimmten Voraussetzungen gemeinsame Dateien errichten. Eine Einschränkung auf bestimmte Daten erfolgt auf gesetzlicher Basis nicht. Regelungen zu Erhebung und Verarbeitung biometrischer Identifizierungsdaten gibt es auch in den einschlägigen Geheimdienstgesetzen nicht; die Befugnis hierzu ist durch die Generalklauseln zur Datenverarbeitung abgedeckt (§ 6 BNDG, § 4 Abs. 1 MADG, § 10 BVerfSchG).

Regelungen, die den **Datenaustausch zwischen Polizei- und sonstigen Exekutivbehörden und Nachrichtendiensten** ermöglichen, müssen den Anforderungen der „hypothetischen Datenneuerhebung“ genügen. Eine Abwägung zwischen dem Verarbeitungszwecke und der Eingriffstiefe für den Betroffenen muss in jedem Fall erfolgen.[22]

10 Anlasslose Erfassung (auch) von Deutschen

Während die biometrische Identifizierung von Ausländern und insbesondere von Flüchtlingen weitgehend etabliert ist, ist die generelle **anlassunabhängige Erfassung** bei Deutschen bzw. der Bevölkerung allgemein erst in jüngster Zeit etabliert worden.

10.1 Registrierung der Bevölkerung

Die Identitätssicherung der Bevölkerung generell und damit also auch der deutschen Staatsangehörigen erfolgt über die **kommunalen Melde-, Personalausweis- und Passbehörden**. Die Meldebehörden haben die in ihrem Zuständigkeitsbereich Wohnenden zu registrieren, um deren Identität und Wohnung feststellen und nachweisen zu können. Sie wirken bei der Durchführung von Aufgaben anderer Behörden oder sonstiger Stellen mit und übermitteln Daten. Zu diesem Zweck führen sie Melderegister (§ 2 BMG). In den dezentralen Melderegistern sind keine biometrischen Daten gespeichert. Gespeichert sind aber – neben anderen Identifizierungsdaten – u.a. nach § 3 Abs. 1 BMG

17. Ausstellungsbehörde, Ausstellungsdatum, letzter Tag der Gültigkeitsdauer und Seriennummer des Personalausweises, vorläufigen Personalausweises oder Ersatz-Personalausweises, des anerkannten Passes oder Passersatzpapiers sowie Sperrkennwort und Sperrsumme des Personalausweises,
17a. die AZR-Nummer in den Fällen und nach Maßgabe des § 10 Absatz 4 Satz 2 Nummer 4 des AZR-Gesetzes.

Damit wird eine Verbindung zur biometrischen Registrierung geschaffen: Innerhalb der **Verwaltungseinheit, der die Meldebehörde angehört**, dürfen alle in § 3 Abs. 1 BMG aufgeführten Daten und Hinweise weitergegeben werden, soweit dies zur Aufgabenerfüllung der jeweiligen Stellen erforderlich ist (§ 37 BMG). Zur gleichen Verwaltungseinheit gehören die Personalausweis- und die Passbehörde sowie die dort geführten Personalausweis- und Passregister.

Mit dem Registermodernisierungsgesetz ist geplant, registerübergreifend die bisherige Steuer-Identifizierungsnummer gemäß § 139b der Abgabenordnung (Steuer-ID) als **nationales Kennzeichen** einzuführen.[23] Die Steuer-ID soll danach ins Melderegister aufgenommen werden (Art. 4, § 3 Abs. 1 Nr. 8 BMG-E), ebenso wie in das Passregister (Art. 7, § 21 Abs. 2 Nr. 9a PassG), in das Personalausweisregister (Art. 8, § 23 Abs. 3 Nr. 9a PAuswG-E) sowie in das Ausländerzentralregister (Art. 6, § 3 Abs. 5 AZRG-E in Bezug auf Flüchtlinge).

10.2 Pass- und Personalausweisgesetz

Das Lichtbild und Fingerabdrücke werden im Pass und im Personalausweis, die Lichtbilder auch im **Passregister** und im **Personalausweisregister** gespeichert. Eine Speicherung der Fingerabdrücke von deutschen Staatsangehörigen findet in diesen **Datenbanken** nicht statt.

Die EU-Mitgliedstaaten stellen auf Basis der Verordnung (EG) 2252/2004 des Rates vom 13.12.2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten **Pässen und Reisedokumenten**, geändert durch Verordnung (EG) 444/2009 vom 28.05.2009, reguläre Reisepässe mit Chip aus, welche das Lichtbild und zwei Fingerabdrücke enthalten. Die europäische Regelung im Jahr 2004 erfolgte auf politischen Druck der Regierung der USA, die mit dem Wegfall der Visumfreiheit für europäische Reisende drohte. Damit werden zwei konkrete Ziele verfolgt: 1. der Schutz vor Fälschung von Pässen und 2. die Verhinderung der betrügerischen Verwendung von Pässen, d.h. deren Verwendung durch andere Personen als ihren rechtmäßigen Inhaber.[24] Deutschland hat den elektronischen Reisepass zum 01.11.2005 und die Speicherung von Fingerabdrücken in Pässen zum 01.11.2007 eingeführt.[25]

Die Verordnung (EU) Nr. 2019/1157 zur Erhöhung der Sicherheit der **Personalausweise** von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben (Perso-VO)[26], schafft zudem europaweit eine einheitliche Rechtsgrundlage für nationale Personalausweise. Gespeichert werden zwei Fingerabdrücke der antragstellenden Person in Form des flachen Abdrucks des linken und rechten Zeigefingers im elektronischen Speicher- und Verarbeitungsmedium des Personalausweises.

Personalausweise werden mit einem hochsicheren Speichermedium versehen, das ein Gesichtsbild des Personalausweisinhabers und zwei Fingerabdrücke in interoperablen digitalen Formaten enthält. Bei der Erfassung der biometrischen Identifikatoren wenden die Mitgliedstaaten die technischen Spezifikationen gemäß dem Durchführungsbeschluss der Kommission C(2018)7767 an (Art. 3 Abs. 5 Perso-VO). Gemäß Art. 3 Abs. 7 Perso-VO waren Kinder unter 6 Jahren sowie Personen, bei denen eine Abnahme von Fingerabdrücken physisch nicht möglich ist, von der Abgabepflicht befreit, Kinder unter 12 Jahren konnten bisher befreit werden.

Das Personalausweisgesetz (PAuswG) regelt die Pflicht zum **Mitführen des Ausweises** und dessen Vorlage bei unterschiedlichen Behörden und sonstigen Stellen (§ 1 Abs. 1 S. 1 PAuswG):

Deutsche im Sinne des Artikels 116 Abs. 1 des Grundgesetzes sind verpflichtet, einen gültigen Ausweis zu besitzen, sobald sie 16 Jahre alt sind und der allgemeinen Meldepflicht unterliegen oder, ohne ihr zu unterliegen, sich überwiegend in Deutschland aufhalten. Sie müssen ihn auf Verlangen einer zur Feststellung der Identität berechtigten Behörde vorlegen und es ihr ermöglichen, ihr Gesicht mit dem Lichtbild des Ausweises abzugleichen.

Bzgl. der **Ein- und Ausreise ins bzw. aus dem Bundesgebiet** besteht in § 1 Abs. 1 PassG eine entsprechende Ausweispflicht durch Vorlage eines Passes.

Die im Chip gespeicherten biometrischen Daten sind nur mit einem hoheitlichen Berechtigungszertifikat **auslesbar**, welches an explizit berechtigte Stellen ausgegeben wird. Die Daten sind durch kryptographische Maßnahmen (Extended Access Control) entsprechend den Vorgaben in der Technischen Richtlinie TR-03110 „Advanced Security Mechanisms for Machine Readable Travel Documents" gegen unberechtigten Zugriff geschützt.[27] Gemäß Art. 11 Abs. 5 VO (EU) 2019/1157 dürfen maschinenlesbare Informationen nur gemäß dieser Verordnung oder dem nationalen Recht des ausstellenden Mitgliedsstaats aufgenommen werden. Erlaubt sind gemäß Art. 11 Abs. 6 VO (EU) 2019/1157 nur die Echtheitsprüfung des Dokuments und die Identitätsprüfung.

Die Aufnahme des Lichtbilds im Personalausweis ist in § 5 Abs. 2 Nr. 5 PAuswG, im Pass in § 4 Abs. 1 S. 1 PassG vorgesehen. Die Fingerabdrücke werden gemäß § 4 Abs. 4 PassG bzw. § 5 Abs. 9 S. 2-4 PAuswG gespeichert:

Die Fingerabdrücke werden in Form des flachen Abdrucks des linken und rechten Zeigefingers des Passbewerbers im elektronischen Speichermedium des Passes gespeichert. Bei Fehlen eines Zeigefingers, ungenügender Qualität des Fingerabdrucks oder Verletzungen der Fingerkuppe wird ersatzweise der flache Abdruck entweder des Daumens, des Mittelfingers oder des Ringfingers gespeichert. Fingerabdrücke sind nicht zu speichern, wenn die Abnahme der Fingerabdrücke aus medizinischen Gründen, die nicht nur vorübergehender Art sind, unmöglich ist.


Bild: iStock.com/Blue Planet Studio

In § 26 Abs. 2 PAuswG bzw. § 16 Abs. 2 S. 3 PassG ist geregelt, dass die bei der Passbehörde gespeicherten Fingerabdrücke spätestens nach Aushändigung des Personalausweises bzw. des Passes **gelöscht** werden müssen.

Das **Passregister und das Personalausweisregister** ist in den §§ 21 ff. PassG und den §§ 23 ff. PAuswG geregelt. In § 21 Abs. 2 PassG sowie § 23 Abs. 3 PAuswG ist vorgesehen, dass neben textlichen Angaben das Passregister sowie das Personalausweisregister ein Lichtbild enthalten darf.

Gemäß § 22a Abs. 2 S. 1-5 PassG u. § 25 Abs. 2 S. 1-4 PAuswG haben die Berechtigung für den automatisierten Abruf des Lichtbildes aus dem Pass- bzw. dem Personalausweisregister Behörden zur Verfolgung von Verkehrsordnungswidrigkeiten sowie generell zur Aufgabenerfüllung: *die Polizeibehörden des Bundes und der Länder, der Militärische Abschirmdienst, der Bundesnachrichtendienst, die Verfassungsschutzbehörden des Bundes und der Länder, Steuerfahndungsdienststellen der Länder, der Zollfahndungsdienst und die Hauptzollämter*.

Die **Zugriffsmöglichkeit von Geheimdiensten** auf die Lichtbilddaten wurde 2017 eingeführt.[28]

11 Abschließende Bewertung

Eine umfassende Bewertung der bestehenden vorstehend dargestellten Regelungen auf europäischer und nationaler Ebene und der Praxis aus Grundrechtssicht ist im Rahmen der hier erfolgenden Darstellung nicht möglich. Folgende **grundsätzliche Kritiken** lassen sich jedoch festhalten:

1. Für die eindeutige Identifizierung mit Hilfe von Fingerabdruckdaten würde der Abdruck eines Fingers genügen. Die Verpflichtung zur Speicherung von 2 Fingerabdrücken bei EU-Bürgern und 10 bei Flüchtlingen verstößt gegen den Grundsatz der Datenminimierung.
2. Die generelle Erlaubnis zur Datennutzung für Sicherheitszwecke bei Daten von Flüchtlingen verstößt gegen den Zweckbindungsgrundsatz.
3. Das in der Praxis bestehende unbegrenzte Zugriffsrecht für Geheimdienste auf Daten von Deutschen und insbesondere von Flüchtlingen ist absolut unverhältnismäßig.
4. Die automatisierte Gesichtserkennung im öffentlichen Raum muss auch künftig unterbleiben.
5. Die Transparenz der Nutzung biometrischer Identifizierungsdaten muss verbessert werden.

Um eine qualifizierte juristische Bewertung insbesondere gemäß dem Verhältnismäßigkeitsgrundsatz vornehmen zu können, bedürfte es zunächst

einer Bestandsaufnahme, in welchem Umfang biometrische Identifizierungsdaten in welcher Art und Weise insbesondere für Sicherheitszwecke genutzt werden und welche Wirkungen dies für die Sicherheit wie für die Rechte der Betroffenen zur Folge hat. Auf der Basis einer solchen **Evaluation der Regelungen** und deren Anwendung ist dann in einem weiteren Schritt eine Überarbeitung der geltenden Bestimmungen unter Berücksichtigung der Grundsätze der Zweckbindung, der Transparenz und der Verhältnismäßigkeit nötig.

Welche praktischen Auswirkungen sich aus einer normativ nicht eingehegten Nutzung biometrischer Identifizierungsdaten ergeben können, demonstrieren uns Überwachungsstaaten wie z.B. China, in denen die biometrische Identifizierung als zentrales Werkzeug zur Unterdrückung und zur Diskriminierung genutzt wird. Wollen wir Zustände wie in China vermeiden, so muss der **demokratische Diskussionsprozess** über die Nutzung biometrischer Identifizierung generell wie insbesondere für staatliche Zwecke intensiviert werden.

Speicherung und Abruf von Fingerabdrücken und Gesichtsbildern

Dateisammlung	**INPOL** (beim BKA)	**SIS/SIS II** (über nationale Zentralen)	**Pass- und Personalausweisregister** (bei den Meldebehörden)	**Pass/Personalausweis**
Art	Gesichtsbild	Fingerabdruck, Gesichtsbild	Gesichtsbild	Fingerabdruck, Gesichtsbild
Zugriff	durch Polizeidienststellen; *automatisiert abgleichbar über das Gesichtserkennungssystem GES*	durch Grenzkontrollbehörden, Justizbehörden, Zoll, Polizei, Geheimdienste; durch Europol und Eurojust zur Gefahren- abwehr/Strafverfolgung	durch Behörden zur Verfolgung von Verkehrsordnungswidrigkeiten; durch Polizei des Bundes und der Länder; durch MAD, BND, Verfassungsschutz des Bundes und der Länder; durch Steuerfahndungsbehörden, Zollfahndung, Hauptzollämter	durch Behörden im In- und Ausland mit hoheitlichem Berechtigungszertifikat

Dateisammlung	**AZR** (beim BAMF)	**VIS** (beim Bundesverwaltungsamt)	**AFIS** (beim BKA)	**Eurodac** (bei nationalen Zentraleinheiten)
Art	Fingerabdruck, Gesichtsbild	Fingerabdruck, Gesichtsbild	Fingerabdruck	Fingerabdruck
Zugriff	durch Asyl- und Ausländerbehörden; durch andere Behörden; insbes. auch durch Polizei und Geheimdienste (2007-2012 auch Lichtbilder der EU-Bürger)	Abruf an Visumsstellen und Außengrenzzugangsstellen; zur Bestimmung der Zuständigkeit für Asylanträge; zur Prüfung des Asylantrags; durch Strafverfolgungsbehörden	durch Polizei; durch Grenz-, Asyl- und Ausländerbehörden	durch BAMF; zentraler Zugriff für Polizei- und Strafverfolgungsbehörden über das BKA

1 BGBl. I 2020 S. 2744.

2 Vgl. Endnote 1.

3 Verordnung (EU) 2016/794 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) v. 11.05.2016, ABl. EU v. 25.06.2016, L 135/53.

4 VO (EG) Nr. 1987/2006 v. 20.12.2006, ABl. EU v. 28.12.2006, L 381/4.

5 Beschluss 2007/533/JI v. 12.06.2007, ABl. EU v. 07.08.2007, L 205/63.

6 VO (EU) 2018/1860, 2018/1861 und 2018/1862 v. 28.11.2018, ABl. EU v. 07.12.2018, L 312/1, L 312/14, L 312/56.

7 Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26.06.2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013, ABl. EU v. 29.06.2013, L 180/1.

8 Verordnung (EG) Nr. 2725/2000 des Rates v. 11.12.2000, ABl. EG v. 15.12.2000, L 316/1.

9 COM (2016) 272 final, 2016/0132 (COD); vgl. COM (2016) 270 final, 2016/0133 (COD).

10 Verordnung (EG) Nr. 767/2008 v. 09.07.2008, ABl. EU v. 15.08.2008, L 218/60.

11 Verordnung (EG) Nr. 810/2009 v. 13.07.2009, ABl. EU v. 15.09.2009, L 243/1.

12 COM(2018) 302 final, näheren Angaben in EU-Kommission v. 24.6.2020, COM(2020) 262 final, S. 4 f.

13 VISZG v. 6.5.2009, BGBl. I S. 1034; zuletzt geändert mit G. v. 19.6.2020, BGBl. I S. 1328, 1332.

14 § 3 (Abs. 1) Nr. 4, 5 AZRG.

15 BGBl. I 2007 S. 1970.

16 BGBl. I 2012 S. 2745.

17 EuGH 16.12.2008 – C-524/06, NVwZ 2009, 378 = DVBl 2009, 171.

18 BGBl. I 2016 S. 130.

19 G. v. 09.01.2002, BGBl. I S- 361, hier Art. 11, 12.

20 Zweites Datenaustauschverbesserungsgesetz (2. DVAG) v. 04.08.2019, BGBl. I S. 1131, Art. 3 Nr. 2 cb, c, Art. 5 Nr. 2.

21 BT-Drs. 19/8752, 68.

22 BVerfG 10.11.2020 – 1 BvR 324/15, Leitsätze 1 und 3a-c.

23 BT-Drs. 19/24226.

24 EuGH 17.10.2013 – C-291/12 Rn. 36, 45, NVwZ 2014, 437 f.

25 BT-Drs. 19/22133, S. 12 f.

26 ABl. EU v. 12.7.2019, L 188/67.

27 BT-Drs. 19/22133, S. 6.

28 Gesetz zur Förderung des elektronischen Identitätsnachweises, G. v. 07.07.2017, BGBl. I S. 2310.

Susanne Holzgraefe

Stempeluhren mit Fingerabdruck-Scanner

Stempeluhren sind umstritten. Manchmal wünschen sich Beschäftigte Stempeluhren bzw. eine genauere Arbeitszeiterfassung, doch der Arbeitgeber oder die Arbeitgeberin ist dagegen. Manchmal ist es umgekehrt.

Der Einsatz von Stempeluhren ist eine Verhandlungssache, beruhend auf individuell zwischen Beschäftigten und Arbeitergeberin bzw. Arbeitgeber vertraglich vereinbarten Anwesenheitszeiten. Gemessen werden darf nur die Anwesenheitszeit und nicht die effektive Arbeitszeit.

Steht die Erledigung von Aufgaben zu bestimmten Terminen und nicht die Präsenz zu bestimmten Zeiten im Vordergrund, so wird i.d.R. Vertrauensarbeitszeit vereinbart. Genaue Festlegungen der Anwesenheitszeit seitens der Arbeitgeberin sind dann nicht zielführend. Doch auch Beschäftigte mit Vertrauensarbeitszeit sind gut beraten die tatsächlich aufgewendete, effektive Zeit zur Erledigung der Aufgabe zur Selbstkontrolle zu erfassen. Die Aufzeichnungen können zur Verhandlungsgrundlage kommender Deadlines oder für Gehaltserhöhungen dienlich sein. Darüber hinaus helfen sie frühzeitig zu erkennen, dass Deadlines nicht eingehalten werden können.

Ist vertraglich eine Anwesenheitspflicht vereinbart, so ist eine präzise Erfassung der Anwesenheitsdauer nötig. Dies ist dann angesagt, wenn Beschäftigte unabhängig vom konkreten Arbeitsanfall anwesend sein sollen. Pförtner, Wachpersonal, Empfangsdamen oder auch Verkaufs- und Gastronomiepersonal können nicht einfach nach Hause gehen, wenn es für eine gewisse Zeit nichts zu tun gibt.

Bei einer Vielzahl von Arbeitsstellen ist eine zeitlich festgelegte Anwesenheitspflicht unumgänglich. In jedem Fall bleibt die Arbeits- und Anwesenheitszeit Verhandlungssache. Die verbindliche Festlegung erfolgt einvernehmlich im Arbeitsvertrag.

Der EuGH prescht vor

Am 14. Mai 2019 entschied der Europäische Gerichtshof (EuGH), dass die gesamte Arbeitszeit erfasst werden muss. Es genügt nicht, wie in Deutschland bisher vorgeschrieben, nur die Mehrarbeit bzw. Überstunden[1] täglich präzise zu erfassen[2]. Arbeitgeberinnen sollen hierfür ein objektives, verlässliches und zugängliches System einrichten, mit dem die tägliche Arbeitszeit jeder Arbeitnehmerin und jedes Arbeitnehmers gemessen werden kann. Wie ein solches System aussehen soll, wurde aber vom Gericht nicht weiter definiert, so dass ein großer Gestaltungsspielraum für die Arbeitgeberinnen bleibt.

Was ist bei der Zeiterfassung zu beachten?

Generell sollte die Erfassung der Arbeitszeit so gestaltet sein, dass sie nicht zur Leistungskontrolle bzw. Leistungsüberwachung verwendet werden kann. Sie sollte sich auf die Erfassung der Anwesenheitszeit inkl. Pausenzeiten beschränken, soweit diese nicht gesetzlich vorgeschrieben bzw. vertraglich vereinbart sind. Außer der Einhaltung der vertraglich vereinbarten Anwesenheitspflichten sollte sich aus der Erfassung erkennen lassen, dass gesetzlich vorgeschriebene Ruhezeiten, gesetzlich vorgeschriebene maximale tägliche bzw. wöchentliche Arbeitszeiten sowie weitere gesetzliche Vorgaben zu Arbeitszeit, Mindestlohn und Arbeitsschutz eingehalten werden.

Die Daten müssen zwei Jahre aufbewahrt werden. Das bedeutet, dass sie nach zwei Jahren unwiderruflich gelöscht werden müssen.

Mitspracherecht Betriebsrat und Datenschutz

Beschäftigte haben ein Mitwirkungs-[3], der Betriebsrat (sofern vorhanden) ein Mitspracherecht, wenn es um die Einrichtung und Verwendung eines Stempeluhrsystems geht.[4] Vor dem Einsatz sollte in jedem Fall (sofern vorhanden) auch die betriebliche Datenschutzbeauftragte zu Rate gezogen werden. Da es sich um die Einführung eines neuen Systems handelt, kann eine Datenschutz-Folgenabschätzung erforderlich sein.

Es sollte ausgeschlossen werden, dass das System zur Leistungskontrolle oder Leistungsüberwachung genutzt werden kann. Des Weiteren sind bei dem Einsatz eines Stempeluhrsystems unter anderem die folgenden Punkte zu beachten:

- Der Zeiterfassungsprozess muss in das Verzeichnis der Verarbeitungstätigkeiten aufgenommen werden.
- Von einer Speicherung außerhalb der EU ist abzuraten.
- Es müssen technische Maßnahmen ergriffen werden, die eine (unabsichtliche) Weitergabe an Dritte und Drittländer ausschließen.
- Alle Beschäftigten sollten in klar verständlicher Art und Weise (Art. 12 DSGVO) transparent entsprechend Art. 13 DSGVO über die Verarbeitung mit dem neuen System informiert werden.
- Es ist genau festzulegen, wer die Daten einsehen und verarbeiten darf.
- Beschäftigte sollten ihre Daten jederzeit selbst einsehen bzw. Kopien der Daten erhalten können.
- Sofern die Zeiterfassung durch ein externes Unternehmen verarbeitet wird, ist ein Auftragsverarbeitungsvertrag abzuschließen.

Stempeluhren mit Fingerabdruck-Scanner

Nehmen wir folgenden Sachverhalt an: Nach einiger Diskussion einigen sich Betriebsrat und Arbeitgeberin auf den Einsatz von Stempeluhren mit Fingerabdruck-Scanner. Der Vorschlag kam in diesem Fall vom Betriebsrat. Der Hersteller des Systems weist aus-


Bild: iStock.com/Iaremenko

drücklich darauf hin, dass das System datenschutzunbedenklich sei.

Alle verlassen gut gelaunt die Sitzung und freuen sich schon auf die neuen Stempeluhren. Doch die betriebliche Datenschutzbeauftragte hat arge Bedenken: Fingerabdrücke zählen zu den biometrischen Daten und gehören damit zu einer besonderen Kategorie personenbezogener Daten, deren Erfassung und Verarbeitung gemäß Art. 9 DSGVO grundsätzlich untersagt ist. Ausnahme: Die betroffene Person hat hier explizit freiwillig eingewilligt.

Hier hat der Betriebsrat, der ja die Beschäftigten in Gänze vertritt, zugestimmt. Darf ein Betriebsrat überhaupt so einfach der Verarbeitung von Daten aus den besonderen Kategorien entsprechend Art. 9 DSGVO zustimmen? Der Betriebsrat hat darüber zu wachen, dass BDSG, DSGVO und andere Gesetze und Verordnungen zum Datenschutz eingehalten werden (§ 80 Abs. 1 Nr. 1 BetrVG). Sofern gegen die Gesetze und Verordnungen des Datenschutzes verstoßen wird, würde die Zustimmung des Betriebsrats seinen in § 80 BetrVG festgelegten Aufgaben widersprechen.

Wenn jeder einzelne Beschäftigte freiwillig einwilligen würde, wäre der Einsatz des Systems zulässig. Ob Freiwilligkeit bei abhängig Beschäftigten gegeben ist, ist immer fraglich. Die Abhängigkeit zur Arbeitgeberin bzw. zum Arbeitgeber und der soziale Druck der Gemeinschaft stehen einer Freiwilligkeit häufig im Wege. Im Fall von Stempeluhren stellt sich bei einem Einsatz mit Erlaubnis durch Einwilligung die Frage: Was passiert, wenn eine Person nicht einwilligt? Was passiert, wenn eine Person die Einwilligung widerruft?

Um dem EuGH-Urteil gerecht zu werden und die komplette Anwesenheitszeit zu erfassen, müsste hier ein paralleles Zeiterfassungssystem eingeführt werden, das die Identifizierung auf einem milderen Weg ermöglicht.

Ist es wirtschaftlich, zwei Systeme parallel zu fahren? Warum nicht gleich für alle ein System einführen, das mildere Mittel verwendet? Immerhin ist ein Grundsatz des Datenschutzes, dass stets das mildeste Mittel einzusetzen ist.

Warum wirbt der Hersteller mit Datenschutz-Unbedenklichkeit?

Das System verarbeitet laut Herstellerdokumenten nicht den ganzen Fingerabdruck, sondern lediglich Fingerlinienverzweigungen (Minutien). Die Datenschutzbeauftragte teilt die Auffassung des Herstellers nicht. In ihren Augen sind auch Minutien biometrische Informationen. Es bleibt Tatsache, dass hier eine Identifizierung über biometrische Daten erfolgt. Ein Urteil des Landesarbeitsgerichts (LAG) Berlin-Brandenburg zeigt, dass die Datenschutzbeauftragte mit ihrer Auffassung nicht alleine ist.

Urteil des LAG Berlin-Brandenburg

Eine Arbeitgeberin aus dem Raum Berlin-Brandenburg setzte ein Stempeluhr-System mit Fingerabdruckscanner ein. Einer der Beschäftigten war damit nicht einverstanden und verweigerte die Nutzung der Stempeluhr. Es kam zur Abmahnung und der Angestellte brachte den Fall vor das Arbeitsgericht. Das hier eingesetzte System verarbeitet nicht den gesamten Fingerabdruck, sondern lediglich die Minutien.

Das LAG Berlin-Brandenburg bestätigte die Auffassung des Angestellten, dass er nicht verpflichtet werden kann, die Stempeluhr zu nutzen.[5] Das Gericht begründet die Entscheidung damit, dass Minutien durchaus biometrische Daten sind, die unter Art. 9 DSGVO fallen, und somit die Verarbeitung zur Identifizierung ausdrücklich untersagt ist. Die Richter konnten nicht erkennen, dass für die Arbeitszeiterfassung zwingend biometrische Daten erforderlich sind.

Fazit

Das LAG Berlin-Brandenburg hält Stempeluhren mit Fingerabdruck-Scanner für nicht zulässig. Das Gericht begründet die Entscheidung damit, dass, selbst wenn nur Teile eines Fingerabdrucks zur Identifizierung verarbeitet werden, es sich trotzdem um biometrische Daten handelt, deren Verarbeitung nach Art. 9 DSGVO explizit untersagt ist. Darüber hinaus sieht das Gericht nicht, dass für eine Arbeitszeiterfassung unbedingt biometrische Daten zur Identifizierung erforderlich sind.

Aus dem Urteil lässt sich schließen, dass nicht nur Stempeluhren mit Fingerabdruck-Scanner unzulässig sind, sondern auch Systeme, welche die Identifizierung mit anderen biometrischen Daten wie Gesichtserkennung, Retina-Scanner usw. vornehmen.

Ein Stempeluhrsystem mit Fingerabdruckscanner für Beschäftigte ist zulässig, wenn jeder einzelne Beschäftigte explizit freiwillig in die Verarbeitung einwilligt. In einem abhängigen Beschäftigungsverhältnis ist die Sicherstellung der Freiwilligkeit schwierig. Um dem EuGH-Urteil gerecht zu werden, muss für Personen, die ihre Einwilligung verweigern, ein milderes System bereitgestellt werden.

Es gibt eine Vielzahl von Angeboten von Stempeluhr-Systemen auf dem Markt, die zur Identifizierung ein milderes Mittel als den Abgleich biometrischer Daten nutzen, um die Anwesenheitszeit von Beschäftigten objektiv und verlässlich zu erfassen, z.B. durch Verwendung von Betriebsausweisen. Eine Identifizierung über biometrische Daten im Rahmen der Arbeitszeiterfassung ist nicht notwendig.

1 Rechtliche Grundlage für Arbeitszeitnachweis für Mehrarbeit bzw. Überstunden ist §16 Abs. 2 ArbZG

2 EuGH Urteil zur Arbeitszeiterfassung vom 14. Mai 2019 mit Aktenzeichen C-55/18

3 Die Mitbestimmungsrechte Beschäftigter ergeben sich aus den §§ 81-84 BetrVG

4 Die Mitbestimmung des Betriebsrates ergibt sich aus § 87 BetrVG

5 Urteil des LAG Berlin-Brandenburg vom 04.06.2020 mit Aktenzeichen 10 Sa 2130/19

Widerstand gegen Entschlüsselungspläne des EU-Rats

Am 14.12.2020 beschloss der Rat der EU unter dem Vorsitz Deutschlands eine Resolution zur Verschlüsselung „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“
https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/de/pdf

Darin fordert der Rat u.a. die „Herstellung des richtigen Gleichgewichts“, wozu gehört, dass es für die Sicherheitsbehörden äußerst wichtig sei, „die Möglichkeit aufrechtzuerhalten, über einen rechtmäßigen Zugang zu Daten für legitime und klar definierte Zwecke im Rahmen der Bekämpfung schwerer und/oder organisierter Kriminalität und Terrorismus – auch in der digitalen Welt – zu verfügen, und die Rechtsstaatlichkeit zu wahren. Bei allen Maßnahmen müssen diese Interessen sorgfältig gegen die Grundsätze der Notwendigkeit, Verhältnismäßigkeit und Subsidiarität abgewogen werden“. Dafür bedürfe es einer „Bündelung der Kräfte mit der Technologiebranche“: „Die zuständigen Behörden müssen unter uneingeschränkter Achtung der Grundrechte und der einschlägigen Datenschutzgesetze rechtmäßig und gezielt auf Daten zugreifen können und gleichzeitig die Cybersicherheit wahren.“

Hierzu erklärte das Netzwerk Datenschutzexpertise:

Der Rat der EU, also die Regierungen der EU-Mitgliedsstaaten, fasst eine Entschließung, wonach Kommunikationsdienste mit einer Ende-zu-Ende-Verschlüsselung, die zunehmend von Betreibern für Jedermann angeboten wird, verpflichtet werden sollen technische Lösungen zum Entschlüsseln durch Polizei und Geheimdienste bereit zu halten und auf Nachfrage herauszurücken. Die Ratsentschließung versucht die Aufregung nach den aktuellen terroristischen Anschlägen zu nutzen, um Sicherheitsbehörden den Zugriff auf technisch gesicherte Kommunikation zu verschaffen. Das Netzwerk Datenschutzexpertise weist darauf hin, dass die Pflicht zum Bereithalten eines Generalschlüssels zum Mitlesen gesicherter Kommunikation verfassungs- und europarechtswidrig wäre.

Angesichts der Bedeutung elektronischer Kommunikation und der Gefahren vor einer Ausspähung dieser Kommunikation durch Kriminelle oder ausländische Geheimdienste, von der US-amerikanischen NSA über den britischen GCHQ bis hin zu chinesischen, russischen oder sonstigen Diensten totalitärer Staaten, hat die Möglichkeit zum Selbstschutz fundamentale Bedeutung zur Wahrung des Telekommunikationsgeheimnisses und des Datenschutzes. Die Pflicht zur Bereitstellung von Zugängen für Sicherheitsbehörden hätte zur Folge, dass dieser Selbstschutz nicht mehr möglich wäre. Es kann nicht gewährleistet werden, dass die Entschlüsselung nur unter rechtsstaatlicher Kontrolle zum Einsatz kommt. Digitale Grundrechte drohen mit einer solchen Maßnahme zum Totalverlust zu werden.

Bürger und Unternehmen hätten kaum noch eine realistische Chance, private oder wirtschaftliche Geheimnisse zu schützen. Der Versuch der Wiederbelebung des seit über 20 Jahren mausetoten „Kanther-Schlüssels“ brächte keinen Schutz, sondern nur Unsicherheit.

Eine Eignung dieser Maßnahme zur Bekämpfung des Terrorismus oder sonstiger schwerer Kriminalität besteht nicht. Kriminelle und Terroristen wären in der Lage, sich Verschlüsselung ohne Hintertüren zu beschaffen; Freiwild würden die rechtschaffenen Menschen, denen der Schutz ihrer Privatsphäre von Bedeutung ist. Freiwild würden auch die Oppositionellen, die in totalitären Staaten mithilfe dieser Technik eine Chance haben, geschützt miteinander zu kommunizieren. Die Pläne gehören wieder auf den Müllhaufen der Geschichte.

#PrivacyIsNotACrime

Folgende Organisationen unterstützen die nachfolgend abgedruckte Stellungnahme zu der Rats-Initiative: Bits und Bäume Dresden, Digitalcourage, Hochschulpiraten Dresden, Komitee für Grundrechte und Demokratie, LabourNet Germany, Partei der Humanisten, Piratenpartei Deutschland, SaveTheInternet, SUMA-EV

Der EU-Ministerrat hat einen raschen Vorstoß unternommen, in dem er Zugriff auf jegliche Kommunikation, auch verschlüsselte, zur besseren Aufklärung von Straftaten fordert. Konkret bedeutet dies, dass beim Einsatz von Verschlüsselungstechnologie, wie sie etwa WhatsApp und Signal anbieten, Generalschlüssel bereitgehalten werden müssen, mit denen jegliche Kommunikation der Nutzenden entschlüsselt werden kann.

Die Privatsphäre der Bevölkerung soll zur angeblichen Terrorbekämpfung geopfert werden, dabei sind die Anschläge der Vergangenheit durch Fehler in der Polizeiarbeit erst möglich geworden. Verschlüsselung ist eine elementare Technologie im Internet, denn sie ermöglicht es Daten vor dem unbefugten Zugriff zu schützen, sei es durch Geheimdienste, Mitbewerber·innen oder Kriminelle. Im Fall von Reporter·innen, Menschenrechtsaktivist·innen oder Whistleblowern kann deren Arbeit oder Leben von Verschlüsselung abhängen. Das Einführen von Generalschlüsseln

stellt ein enormes Sicherheitsrisiko dar, da diese von allen verwendet werden können, die Zugriff auf sie haben. Eine derart geschwächte Verschlüsselung wäre damit de facto wertlos. Ein Verbot sicherer Verschlüsselung ließe sich außerdem von versierten Akteur·innen umgehen, indem vorhandene, sichere Verschlüsselungstechnik auf privaten Diensten genutzt wird.

Wir fordern daher einen sofortigen Stopp der Verhandlungen auf europäischer Ebene. Vorhandene Befugnisse die das Umgehen von Verschlüsselungen ermöglichen, wie etwa Staatstrojaner, müssen EU-weit untersagt werden. Weiter fordern wir eine europäische Initiative für ein Grundrecht auf Verschlüsselung.

Weitere Infos unter:
https://privacyisnotacrime.eu/de

Gemeinsame Pressemitteilung der Bürgerrechtsorganisation Humanistische Union mit weiteren NGOs vom 23.11.2020

Verfassungsbeschwerde gegen Trojaner-Einsatz durch Verfassungsschutz und Predictive-Policing-Befugnisse der Polizei in Hamburg

GFF bereitet mit Klage auch Vorgehen gegen Änderung des Artikel 10-Gesetzes auf Bundesebene vor

Der Hamburger Verfassungsschutz und die Polizei verfügen seit April 2020 über scharfe Überwachungsinstrumente: Der Verfassungsschutz darf mit Trojanern verschlüsselte Kommunikation ausforschen, die Polizei mittels Algorithmen Personenprofile erstellen. Die Humanistische Union, die Gesellschaft für Freiheitsrechte e.V. (GFF) und weitere NGOs erheben heute Verfassungsbeschwerde gegen die entsprechenden Gesetzesänderungen. „Angesichts der umstrittenen Überwachungspraxis von Geheimdiensten und wiederkehrender Polizei-Skandale sind neue Befugnisse für diese Behörden höchst bedenklich. Wie diese Befugnisse in Hamburg geregelt sind, ist darüber hinaus verfassungswidrig“, sagt Bijan Moini, Jurist und Verfahrenskoordinator bei der GFF.

Geheimdiensttrojaner verletzt Grundrechte

Seit einer Änderung des Hamburgischen Verfassungsschutzgesetzes im April 2020 darf sich das Hamburger Amt für Verfassungsschutz ohne Gerichtsbeschluss oder ähnliche Vorab-Kontrolle in Geräte bestimmter Personen hacken (§ 8 Abs. 12). Das verletzt Betroffene in ihrem IT-Grundrecht (Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme) und es verletzt ihr Telekommunikationsgeheimnis. Zudem gefährdet der Geheimdiensttrojaner die vertrauliche Kommunikation von Berufsgeheimnisträgern wie Anwält*innen und Journalist*innen und verletzt damit insbesondere die Pressefreiheit. „Mit dem Geheimdiensttrojaner sind nun selbst verschlüsselte Nachrichten nicht mehr sicher“, sagt Sebastian Friedrich, einer der Kläger*innen. „Das erschwert meine Arbeit ungemein: Es ist mir kaum möglich, wegen einer kurzen Nachfrage einmal quer durch Deutschland zu fahren, um mit meinem Kontakt face-to-face zu reden.“ Friedrich arbeitet als freier Journalist u.a. für den NDR und recherchierte in der Vergangenheit zur militanten Rechten und zum Rechtsterrorismus. Viele seiner Informant*innen brauchen besonderen Schutz.

Hamburger Regelungen zum Trojaner-Einsatz sind verfassungswidrig

Trojaner in Händen von Geheimdiensten sind verfassungswidrig, wenn ihr Einsatz nicht hinreichend begrenzt ist und der Staat Sicherheitslücken in IT-Systemen ausnutzt, statt sie den Betreibern zu melden. All das ist in Hamburg der Fall. Zudem urteilte das Bundesverfassungsgericht nach einer Verfassungsbeschwerde der GFF gegen die Auslandsüberwachung durch den Bundesnachrichtendienst im Mai 2020, dass die heimliche Überwachung bestimmter Personen einer gerichtsähnlichen Vorab-Kontrolle unterliegen muss. „In Hamburg werden die Überwachungsbefugnisse deutlich erweitert ohne das Kontrollregime zu verbessern – damit ist der Verfassungsverstoß programmiert“, sagt Moini.

Hamburger „Predictive Policing“-Ansatz ist verfassungswidrig

Die Verfassungsbeschwerde richtet sich außerdem gegen die automatisierte Auswertung von Daten durch die Hamburgische Polizei (§ 49 HmbPolDVG). Die Polizei darf automatisierte Personenprofile aus einer nicht näher bestimmten Menge an Daten erstellen, darunter ggf. auch öffentlich verfügbare Daten aus sozialen Netzwerken. Es ist unklar, von wem Profile angefertigt werden können und welche Konsequenzen etwaiger „Beifang“ für die Betroffenen hat, also die Erfassung von Personen, die selbst nicht als gefährlich gelten. Unklar ist auch, für welche Zwecke genau Software eingesetzt werden kann und wie lange die Profile gespeichert

werden. In Hamburg soll dadurch die vorbeugende Verbrechensbekämpfung („Predictive Policing“) Einzug halten – allerdings unter Verletzung der Grenzen, die das Bundesverfassungsgericht der weniger eingriffsintensiven Rasterfahndung gesetzt hat.

Bund will Nachrichtendienste deutschlandweit mit Trojanern ausstatten

Die Verfassungsbeschwerde steht in einem bundespolitischen Zusammenhang: Die Große Koalition will das Artikel 10-Gesetz kurzfristig ändern und alle Verfassungsschutzbehörden sowie weitere Nachrichtendienste mit Trojanern ausstatten. Die Reformpläne leiden an den gleichen Mängeln wie das Hamburgische Verfassungsschutzgesetz. „Unsere Beschwerde gegen das Hamburger Gesetz ist ein Musterverfahren für die Reform auf Bundesebene: Wir wollen die mit dem Geheimdiensttrojaner verbundenen Grundsatzfragen frühzeitig durch das Bundesverfassungsgericht klären lassen“, sagt Moini.

Die GFF koordiniert die Verfassungsbeschwerde. Initiiert wurde und unterstützt wird sie von der Humanistischen Union Hamburg, den Kritischen Jurastudierenden Hamburg, der Vereinigung Demokratischer Juristinnen und Juristen und der Deutschen Journalistinnen- und Journalisten-Union (dju). Zu den Kläger*innen zählen die Rechtsanwältin Britta Eder sowie Aktivist*innen und Journalist*innen, darunter Sebastian Friedrich (NDR u.a.) und Katharina Schipkowski (taz). Sie werden vertreten durch Jun.-Prof. Dr. Sebastian Golla (Ruhr-Universität Bochum).

Weitere Informationen zur Verfassungsbeschwerde finden Sie unter: https://freiheitsrechte.org/verfassungsbeschwerde-polizei-verfassungsschutzgesetz-hh

Pressemitteilung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz vom 07.12.2020

Souveränität der Versicherten bei der elektronischen Patientenakte bewahren und Gesundheitsdaten konsequent schützen – Kugelmann appelliert an Krankenkassen und Gesetzgeber

Die Digitalisierung im Gesundheitswesen schreitet immer schneller voran. Die Bundesregierung forciert den zuvor jahrelang nur schleppend vorangekommenen Prozess der digitalen Transformation des deutschen Gesundheitswesens durch zahlreiche Gesetzgebungsvorhaben. Nachdem erst im Oktober 2020 das Patienten-Datenschutzgesetz (PDSG) in Kraft getreten ist, hat das Bundesgesundheitsministerium Mitte November bereits den nächsten Entwurf vorgelegt, diesmal für ein „Gesetz zur digitalen Modernisierung von Versorgung und Pflege“, kurz DVPMG genannt. Aus der Perspektive des Datenschutzes ist der digitale Umbau des Gesundheitssystems in Deutschland zu begrüßen, sofern auch in der digitalen Versorgung die Souveränität der Versicherten hinsichtlich der Verarbeitung ihrer Daten bewahrt und deren Schutz konsequent sichergestellt wird. Doch daran hapert es immer wieder, wie die zwei aktuellen Beispiele zeigen:

Bei der mit dem Patienten-Datenschutzgesetz zum Jahresanfang 2021 etablierten elektronischen Patientenakte wird den Versicherten ohne geeignetes Endgerät die Wahrnehmung der ihnen zustehenden Rechte in unzumutbarer Weise erschwert. Im Jahr 2021 besteht gar keine Möglichkeit, ohne eigenen PC, Handy oder Tablet in die Inhalte der eigenen Akte Einblick zu nehmen und Zugriffsrechte darauf zu steuern. Ab 2022 kann ein Vertreter benannt werden, über den dies dann möglich sein soll. Eine unmittelbare Rechteausübung ist zu keinem Zeitpunkt vorgesehen. „Damit werden Versicherten ihnen unmittelbar zustehende elementare Datenschutzrechte genommen. Mit der Aufstellung eigener Terminals bei den Krankenkassen oder anderen geeigneten Maßnahmen hätte man dies vermeiden können und müssen“, konstatiert der rheinland-pfälzische Landesdatenschutzbeauftragte Professor Dieter Kugelmann. „Die gesetzlichen Vorgaben missachten in grober Weise die den Versicherten zustehende Wahrnehmung ihres Grundrechts. Sollten sich Betroffene an mich wenden und Defizite bei der Ausübung ihrer Rechte geltend machen, werde ich von den meiner Aufsicht unterliegenden Krankenkassen verlangen, dass die Versicherten ihre Datenschutzrechte unmittelbar ausüben können.“

Auch in Bezug auf den neuesten Gesetzentwurf aus dem Bundesgesundheitsministerium sieht der Landesdatenschutzbeauftragte Verbesserungsbedarf. Mit dem Entwurf des DVPMG wird die Digitalisierung im Gesundheitswesen vertieft und auf den Bereich der Pflegeversicherung ausgeweitet. Doch es gibt deutliche Defizite: So sollen digitale Gesundheits- und Pflegeanwendungen unter anderem noch bis zum Jahr 2023 erstattungsfähig sein, wenn deren Datenschutz- und Sicherheitstauglichkeit allein von den Herstellern selbst erklärt wird. Erst danach bedarf es im Hinblick auf die Sicherheit der Anwendungen

der Vorlage von Zertifikaten; bezüglich des Datenschutzes ist das auch danach nicht vorgesehen. Kugelmann sagt: „Dem Schutz der Gesundheitsdaten, die in den digitalen Anwendungen sowohl in der Krankenversorgung als auch der Pflege verarbeitet werden, muss höchste Priorität beigemessen werden. Allein den eigenen Erklärungen der Hersteller zu vertrauen, darf als Nachweis für die Einhaltung der Anforderungen an den Datenschutz und die Datensicherheit nicht ausreichen. Schon die Zulassung der ersten digitalen Gesundheitsanwendungen hat dies eindrucksvoll gezeigt.“ Kugelmann betont weiter: „Ich appelliere deshalb an den Gesetzgeber, ausschließlich den Einsatz von sicheren und datenschutzgerechten Anwendungen sicherzustellen und dabei die in dem Datenschutzrecht vorhandenen Möglichkeiten der Zertifizierung im besonders sensiblen Gesundheitswesen zu nutzen und dies nicht erst im Jahr 2023, sondern sofort. Datenschutz und IT-Sicherheit dürfen nicht auf die lange Bank geschoben werden.“

In seiner gegenüber der Landesregierung zu dem Gesetzentwurf abgegebenen Stellungnahme fordert Professor Dieter Kugelmann weiter, bei der im Gesetz vorgesehenen Einrichtung eines zentralen Kommunikationsdienstes für das Gesundheitswesen die Vorgaben des Datenschutzes für die Nutzung von E-Mail- und Messaging-Diensten zu beachten und insbesondere die Nutzung privater Endgeräte zur Kommunikation im beruflichen Kontext zu verbieten. Die Einrichtung einer Schweigepflicht für Hersteller von digitalen Gesundheits- und Pflegeanwendungen begrüßte er, wobei sich diese auf alle an der Herstellung und den Betrieb mitwirkenden Personen erstrecken sollte.

Pressemitteilung der Gesellschaft für Informatik (GI) und vieler weiterer Organisationen vom 18.12.2020

Offener Brief: Ausreichende Fristen für Verbändebeteiligung*

Wirkliche demokratische Mitsprache statt Beteiligungssimulation – Verbände und zivilgesellschaftliche Akteure fordern auf Initiative der Gesellschaft für Informatik e.V. längere Fristen zur Kommentierung von Gesetzentwürfen und einen offeneren Beteiligungsprozess.

Die Gesellschaft für Informatik e.V. (GI) und mehr als ein Dutzend weiterer Vereine und Verbände richten sich in einem offenen Brief „Angemessene Fristen statt Scheinbeteiligung“ an alle Bundesministerinnen und -minister. Sie fordern darin insbesondere angemessene Fristen für die Kommentierung von Gesetzesentwürfen.

Im Dezember wurde mit einer 28-Stunden-Frist für Stellungnahmen zum Vierten Referentenentwurf des IT-Sicherheitsgesetzes 2.0 (108 Seiten) und einer 48-Stunden-Frist zur Novellierung des Telekommunikationsgesetzes (465 Seiten) ein Tiefpunkt der bundesdeutschen Verbändebeteiligung erreicht.

GI-Geschäftsführer Daniel Krupka: „Wer ernsthaftes Interesse an der Beteiligung der Zivilgesellschaft und Verbänden am Gesetzgebungsprozess hat, muss auch für Rahmenbedingungen sorgen, die dies ermöglichen. In solch kurzer Zeit ist eine ernsthafte Beteiligung insbesondere zivilgesellschaftlicher Akteure schlichtweg nicht möglich. Deshalb fordern wir eine wirkliche und auch für Vereine und Verbände umsetzbare Beteiligung, statt der Simulation von Partizipation, die wir in letzter Zeit immer öfter erleben durften.“

Die Beteiligung von Zivilgesellschaft und Verbänden an Gesetzgebungsprozessen ist ein elementarer Bestandteil unserer Demokratie. Deshalb ist in § 47 der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO) auch eine „möglichst frühzeitige“ Zuleitung an Verbände vorgesehen. In der Realität sieht es allerdings häufig so aus, dass Stellungnahmen zu Gesetzesvorschlägen in weniger als drei Arbeitswochen – teilweise von gerade einmal wenigen Werktagen – erwartet werden.

Die Unterzeichner*innen – Verbraucherzentrale Bundesverband e. V., Transparency International Deutschland e.V., Stiftung Neue Verantwortung, eco – Verband der Internetwirtschaft e. V., Bundesverband IT-Mittelstand e.V. (BITMi), Chaos Computer Club (CCC), u.v.a. – fordern längere Kommentierungsfristen von mindestens vier Arbeitswochen sowie eine Orientierung an der Länge eines Gesetzentwurfes. Wir schlagen vor: Pro 50 Seiten, je eine Woche Bearbeitungszeit.

Neben längeren Fristen fordern die Unterzeichner*innen die Bereitstellung von Synopsen, die Veröffentlichung der Referentenentwürfe sowie eine Öffnung des Kommentierungsprozesses.



Bild: iStock.com/djenkaphoto

Pressemitteilung vom 09.02.2021

Deutsche Vereinigung für Datenschutz gegen ARZG-Änderung

Vor wenigen Tagen stellte das Bundesinnenministerium (BMI) im Rahmen einer Verbändeanhörung einen Referentenentwurf für die Änderung des Gesetzes zum Ausländerzentralregister (AZR, AZRG) vor. Damit will das Ministerium die Digitalisierung im Ausländer- und Asylwesen verbessern. Geplant ist die Datenbestände zwischen dem AZR und weiteren mit Ausländern befassten Behörden zu „synchronisieren“. Dafür ist u.a. vorgesehen, dass im AZR von Ausländern vorgelegte Dokumente sowie behördliche Entscheidungen über Asyl, Aufenthalt, Einreisebedenken oder politisches Betätigungsverbot vorgehalten werden, um sie bei Bedarf kurzfristig digital zu übermitteln. Außerdem ist geplant im AZR ausländische Personenidentitätsnummern aufzunehmen, die nicht nur zur Identifizierung genutzt werden können, sondern auch zum Datenaustausch zwischen deutschen und Heimatbehörden. Obwohl die Wohnadressen schon in den Melderegistern gespeichert sind, sollen sie für Nicht-EU-Bürger künftig auch ins AZR aufgenommen und generell zum Abruf bereitgestellt werden.

Der Entwurf plant eine Ausweitung der behördlichen Befugnisse ohne aber auch nur an einer Stelle die Transparenz für die Betroffenen und deren Möglichkeit, rechtliches Gehör zu erhalten, zu verbessern. Da es sich hier um hochsensible Informationen handelt, die Auskunft über politische Verfolgung, über prekäre Familienverhältnisse oder über Notsituationen geben, wird sowohl vom Verfassungsrecht wie von der europäischen Datenschutz-Grundverordnung gefordert, dass ein solches Gesetz Schutzvorkehrungen für die Betroffenen vorsieht.

Dazu der DVD-Vorsitzende Frank Spaeing: „Das Gesetz zum AZR müsste generell wegen Datenschutzverstößen umfassend überarbeitet werden. Statt die Rechte der Betroffenen auf den europaweit geltenden Standard zu bringen, wird mit dem BMI- Entwurf die Entrechtung und Bevormundung der Ausländer weiter vorangetrieben. Der Entwurf darf so nicht Gesetz werden.“

Der stellvertretende DVD-Vorsitzende Werner Hülsmann ergänzt: „Die vom Innenministerium durchgeführte Verbändeanhörung war eine Farce: Soweit bekannt, wurde kein Datenschutzverband beteiligt, obwohl es im Entwurf durchgängig um verschärfte Dateneingriffe geht. Und eine Frist von 4 Tagen zur Stellungnahme auf einen über 100-seitigen Gesetzentwurf verhindert, dass sich Experten qualifiziert mit einer derart schwerwiegenden Gesetzesänderung auseinandersetzen können.“


Von den Jahren 2014 und 2015 sind noch alle Hefte in großer Anzahl verfügbar
Bestellbar für 4 Euro pro Jahrgang oder 6 Euro für beide Jahrgänge *
Datenschutz Nachrichten
1/2014 Konzern-Datenschutz
2/2014 Das Internet der Dinge
3/2014 Datenschutz im Reiseverkehr
4/2014 Big Data
1/2015 Mobilität, Telematik und Datenschutz
2/2015 Datenerfassung und Flüchtlinge
3/2015 Rote Linien zur EU-DSGVO
4/2015 Sichere Häfen
* Nur solange der Vorrat reicht

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Anti-Pandemiegesetz stärkt Datensammelei durch RKI

Das am 18.11.2020 von Bundestag und Bundesrat verabschiedete und kurz danach in Kraft gesetzte „Dritte Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite“ (kurz Drittes Bevölkerungsschutzgesetz) sieht eine zentralisierte Konsolidierung von Patientendaten bei einer Bundesbehörde vor.

Gemäß den weitreichenden Änderungen des Infektionsschutzgesetzes (IfSG) durch die Große Koalition wird unter anderem eine neue zentrale Sammelstelle für digitale Personendaten beim Robert-Koch-Institut (RKI) eingerichtet. Das RKI wird neben Meldedaten zu SARS-CoV-2-Infektionen demnach auch Patientendaten zu allen Impfungen gegen das Coronavirus und über die Reisebewegungen deutscher und ausländischer Bürger erhalten. Das deutsche elektronische Melde- und Informationssystem für den Infektionsschutz (DEMIS) ist laut RKI eine Weiterentwicklung des bestehenden Systems zur Verarbeitung von Krankheitsmeldungen nach dem IfSG. Mit dem neuen Gesetz werden nun alle meldepflichtigen Stellen veranlasst, ihre Daten an dieses System zu übermitteln.

Neben den üblichen Patienten- und Kontaktdaten müssen jetzt auch die lebenslange Arztnummer (LANR) des behandelnden Arztes und die Betriebsstättennummer (BSNR) seiner Gesundheitseinrichtung übermittelt werden. Zusätzlich wird die Ortsangabe bei der Übermittlung der Daten von Infizierten präzisiert. Außerdem sollen die Daten von Patienten an das RKI geschickt werden, die Impfungen gegen das SARS-CoV-2-Virus erhalten. Das soll in pseudonymisierter Form erfolgen und dient der Überprüfung der Wirksamkeit der Impfstoffe durch das Robert-Koch-Institut und das Paul-Ehrlich-Institut (PEI). Obwohl das PEI für die Zulassung und Prüfung von Impfstoffen zuständig ist, lagern die Daten im DEMIS beim RKI. Weiterhin erhält das RKI nun auch Daten über Personen, die aus Risikogebieten in die Bundesrepublik einreisen und stichprobenartig von Bundesbürgern, die eine Bundesgrenze übertreten.

Die Kontrolle dieser Maßnahmen nach datenschutzrechtlichen Gesichtspunkten liegt beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) Ulrich Kelber (SPD). Datenschutzbeauftragte der Länder sind außen vor.

Kelber kritisierte in seiner zuvor erstellten Stellungnahme: „Erneut werden mit dem Gesetz verschiedene Meldepflichten oder Übermittlungen personenbezogener Daten eingeführt oder erweitert, ohne zu berücksichtigen, dass die Verarbeitung von Gesundheitsdaten, also besonders geschützten personenbezogenen Daten, einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt und daher sorgfältig zu begründen und zu rechtfertigen ist und besondere flankierende Maßnahmen zum Schutz der sensiblen Daten vorzusehen sind.“

Der BfDI kritisierte die Hast, mit der das Gesetz vorgelegt und verabschiedet wurde. Das habe es kaum möglich gemacht zu prüfen, ob es datenschutzrechtlich unbedenklich ist. Eine ganze Reihe von Vorschlägen Kelbers, die Datensammlung einzuschränken oder etwa die Nutzung der Daten und deren Empfänger zu präzisieren, wurde nicht berücksichtigt. Zur Erhebung von Pandemiedaten durch das RKI meint Kelber in der Stellungnahme: „Allgemein sehe ich mit Besorgnis, dass die Gewinnung von Erkenntnissen zunehmend gesetzlich vorgesehen und bundesweit zwingend durch staatliche Stellen vorgesehen wird. Dies übergeht die in Deutschland durchaus vorhandenen Möglichkeiten klinischer und wissenschaftlicher Forschung, die einwilligungsbasiert erfahrungsgemäß zuverlässige Ergebnisse liefert.“

Kelber war nicht direkt in den Entwurf oder wenigstens zeitnah in die Änderungen des Dritten Bevölkerungsschutzgesetzes eingebunden: „Diese extrem kurzen Fristen erschweren eine sachgerechte Bearbeitung erheblich und erscheinen zu einem Zeitpunkt, zu dem die Pandemie-Lage seit mehr als sieben Monaten besteht, nicht angemessen.“ Die Geschwindigkeit, in der das entsprechende Gesetz verfasst und dem Bundestag und dem Bundesrat zur Abstimmung vorgelegt wurde, wurde auch von einer Reihe von Abgeordneten der Opposition ausdrücklich bemängelt.

Obwohl Melde- und Gesundheitsdaten in Deutschland grundsätzlich nicht auf der Ebene des Bundes erfasst oder gespeichert werden, institutionalisierte das IfSG zum 01.01.2001 das Robert-Koch-Institut als neue Bundesbehörde für die Erfassung und Speicherung von Patienten- und Gesundheitsdaten im Zusammenhang mit meldepflichtigen Krankheiten. Diese Rolle wird mit der erfolgten Überarbeitung des Gesetzes verstärkt. Die Daten von Personen, die an COVID-19 erkrankt sind, mit dem SARS-CoV-2-Virus infiziert wurden oder in Verdacht stehen infiziert worden zu sein oder andere anstecken zu können, werden somit nun direkt an das RKI übermittelt. Dazu zählen auch die Daten von Personen, die nach Deutschland einreisen oder einreisen wollen.

Private Beförderer (etwa im öffentlichen Personennahverkehr, die Deutsche Bahn und Fluggesellschaften) müssen eine Reihe von Gesundheitsdaten, Impfdokumente, Testergebnisse und Angaben zu Symptomen erheben und übermitteln. Gleiches gilt für die Bundespolizei und andere Polizeibehörden, die zusätzlich bei Nichtvorhandensein von Impf- oder Testdokumenten eine entsprechende grenzübertretende

Person zur Durchführung eines Tests auf SARS-CoV-2 (gemeint ist hier wohl aktuell eine Feststellung per Nasenabstrich und RT-PCR) zwingen kann. Hinzu kommen die (pseudonymisierten) Daten all jener Patienten, die einen Impfstoff gegen das SARS-CoV-2-Virus erhalten. Das Robert-Koch-Institut erhält so in Zukunft die Daten von Millionen von Bundesbürgern. Die neue Gesundheits-Cloud DEMIS wird zur Speicherung und Analyse dieser Daten vom RKI betrieben und zusammen mit der Gesellschaft für Telematik (Gematik) entwickelt, die auch für die elektronische Patientenakte (ePA) zuständig ist (Scherschel, Drittes Bevölkerungsschutzgesetz: Massenhafte Datenspeicherung beim RKI, www.heise.de 19.11.2020, Kurzlink: https://heise.de/-4964944).

Bund

Kelber kritisiert Nichtumsetzung der Datenschutzrichtlinie für Polizei und Justiz

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Ulrich Kelber hat festgestellt, dass Deutschland in den Bereichen des Datenschutzes bei Polizei und Justiz weiter massiv hinterherhinkt und deshalb die Bundesregierung aufgefordert, die einschlägige EU-Richtlinie von 2016 (DSRl-JI) vollständig umzusetzen. Die EU-Mitgliedsstaaten hatten sich verpflichtet alle dafür notwendigen Gesetze bis zum 06.05.2018 zu erlassen. Deutschland habe diese Frist am 29.01.2021 schon um 1000 Tage überschritten.

Kelber kann als BfDI Datenschutzverstöße bei der Bundespolizei und der Zollfahndung momentan „nur beanstanden": „Ohne nationale Gesetze fehlen mir wirksame Durchsetzungsbefugnisse. Das untergräbt die demokratische Legitimation der Datenschutzaufsicht und der Strafverfolgungsbehörden gleichzeitig." Der Informatiker sieht den Gesetzgeber daher „sofort" zum Handeln verpflichtet. Im Frühjahr 2020 habe seine Behörde zwar den Entwurf eines neuen Bundespolizeigesetzes erhalten, mit dem auch Vorgaben aus der DSRl-JI berücksichtigt worden wären. Dieser sei bisher jedoch nicht in den Bundestag gelangt. Die Bundesregierung wollte die Initiative, mit der die Ermittler auch den Bundestrojaner etwa zum Hacken von Smartphones und Laptops einsetzen können sollen, eigentlich im Januar 2021 auf den Weg bringen. Das Vorhaben war aber aufgrund des Streits zwischen einzelnen Ressorts nicht mehr im Plan.

Das Zollfahndungsdienstegesetz hat der Gesetzgeber zwar bereits umfassend überarbeitet. Bundespräsident Frank-Walter Steinmeier (SPD) unterzeichnete es aber wegen der enthaltenen verfassungswidrigen Klauseln zur Bestandsdatenauskunft noch nicht. Der Gesetzgeber hätte Kelber zufolge stattdessen auch eine Änderung im dritten Teil des Bundesdatenschutzgesetzes (BDSG) vornehmen können, um die Regeln nicht für jede Behörde in Fachgesetzen wiederholen zu müssen. Immerhin ist, so Kelber, die Richtlinie für den Bereich des Bundeskriminalamtes (BKA) grundsätzlich umgesetzt. Im BKA-Gesetz habe der Bundestag geregelt, dass die Aufsichtsbehörde geeignete Abhilfemaßnahmen anordnen kann, „wenn dies zur Beseitigung eines erheblichen Verstoßes gegen datenschutzrechtliche Vorschriften erforderlich ist". Anordnungsbefugnisse fehlten aber ferner im Bereich der Geheimdienste, sodass auch hier derzeit nur ein Beanstanden möglich ist.

Bei der DSRl-JI handelt es sich um den „kleinen Bruder" der stärker im öffentlichen Fokus stehenden Datenschutz-Grundverordnung (DSGVO). Der „Zwilling" schützt das Grundrecht der Bürger auf Privatheit, wenn Strafverfolgungsbehörden personenbezogene Daten verwenden. Die enthaltenen EU-Vorschriften sollen mit ähnlichen Betroffenenrechten wie in der DSGVO gewährleisten, dass die personenbezogenen Informationen von Opfern, Zeugen und Verdächtigen angemessen geschützt werden (dazu DANA 1/2016, 8 ff.). Die EU-Kommission leitete in der Sache im Mai 2020 die zweite Stufe eines Vertragsverletzungsverfahren gegen Deutschland ein. Sie monierte dabei auch, dass fünf der 16 Bundesländer noch keine Maßnahmen ergriffen haben, um die Bestimmungen umzusetzen. Die damals gesetzte Frist ist im Herbst abgelaufen, sodass die Kommission in Brüssel den Fall nun an den Europäischen Gerichtshof verweisen kann (Krempl, Polizei & Justiz: EU-Datenschutzrichtlinie seit 1000 Tagen nicht umgesetzt, www.heise.de 30.01.2021, Kurzlink: https://heise.de/-5041277).

Bund

StPO-Verschärfung mit Kfz-Kennzeichenscanning geplant

Die Bundesregierung plant gemäß einem Kabinettsbeschluss vom 20.01.2021 eine „Fortentwicklung der Strafprozessordnung" (StPO). Damit sollen Polizei und andere Sicherheitsbehörden wie der Zoll u.a. eine einheitliche Rechtsgrundlage für den Einsatz automatisierter Kennzeichenlesesysteme (AKLS) im öffentlichen Verkehrsraum zu Fahndungszwecken erhalten. Gemäß dem geplanten § 163g StPO dürfen Strafverfolger „örtlich begrenzt im öffentlichen Verkehrsraum" ohne das Wissen der betroffenen Personen „Kennzeichen von Kraftfahrzeugen sowie Ort, Datum, Uhrzeit und Fahrtrichtung durch den Einsatz technischer Mittel automatisch" erheben. Die Daten können anschließend abgeglichen werden mit Kfz-Kennzeichen, die auf den Beschuldigten oder auf Verbindungspersonen zugelassen sind oder von ihnen genutzt werden. Im Referentenentwurf des Bundesjustizministeriums war zunächst ein allgemeinerer Abgleich mit „Halterdaten" vorgesehen.

Für das Kennzeichen-Scanning müssen „zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass eine Straftat von erheblicher Bedeutung begangen worden ist". Der weitgehend unbestimmte Rechtsbegriff bezieht sich auf gewerbs-, gewohnheits-, serien-, bandenmäßig und allgemein „organisiert" begangene Straftaten. Dazu zählen auch Betrugsfälle, Drogenkriminalität und das Verbreiten von Darstellungen sexuellen Kindesmissbrauchs. Das Kennzeichen-Scanning soll zulässig sein, wenn es „zur Ermittlung der Identität oder des Aufenthaltsorts des Beschuldigten führen kann". Dies soll auch gelten, wenn das Kennzeichen des mutmaßlichen Tä-

ters bekannt ist, der Name eines Flüchtigen aber noch nicht. Die Daten dürfen laut Gesetzentwurf „nur vorübergehend und nicht flächendeckend“ automatisiert erhoben werden. Wenn kein Treffer vorliegt oder dieser nicht bestätigt werden kann, müssten die erhobenen Informationen „sofort und spurenlos“ gelöscht werden.

Eine schriftliche Anordnung „der Staatsanwaltschaft oder ihrer Ermittlungsperson“ soll ausreichen. Darin müssen die Halterdaten der Verdächtigen und die Stellen der Überwachung genau bezeichnet werden. Bei Gefahr im Verzug ist eine mündliche Anweisung möglich. Die Anordnung muss befristet werden, ein Richtervorbehalt sei nicht angezeigt.

Für die Gefahrenabwehr ist das Kennzeichen-Scanning schon seit vielen Jahren anlassbezogen polizeirechtlich in zahlreichen Bundesländern erlaubt. Bisher wurde das Instrument im Rahmen der Strafverfolgung auf § 100h StPO gestützt, was aber rechtliche Unsicherheiten zur Folge hatte. Diese Regelung erlaubt, dass „auch ohne Wissen der betroffenen Personen außerhalb von Wohnungen Bildaufnahmen hergestellt werden dürfen“, um den Aufenthaltsort eines Beschuldigten herauszufinden. Nicht abgedeckt ist das Abgleichen von Kennzeichen mit Datenbanken. Vor allem in Brandenburg ist die Nummernschilderfassung sehr umstritten, eine Verfassungsbeschwerde ist anhängig (DANA 2/2020, 119 f.; DANA 2/2019, 92 f.).

Vom Kennzeichen-Scanning sind typischerweise viele Personen betroffen Diese alle anschließend über den Grundrechtseingriff zu benachrichtigen erscheint der Bundesregierung „praktisch undurchführbar“ und sei verfassungsrechtlich auch nicht vorgeschrieben. Informiert werden sollen daher nur Beschuldigte und Kontaktpersonen.

• Kritik

Rena Tangens vom Datenschutzverein Digitalcourage erwartet, dass auch die nun geplante bundesweite Erlaubnis vor dem Bundesverfassungsgericht keinen Bestand haben dürfte. Schon 2008 habe das höchste Gericht klargestellt, dass es enge Grenzen für die Verhältnismäßigkeit bei diesem Instrument gebe. Mit der vorgesehenen StPO-Novelle bleibe aber vieles vage: So sollten Kfz-Kennzeichen „vorübergehend“ und „örtlich begrenzt“ beim Verdacht auf „erhebliche Straftaten“ erlaubt werden, was den Behörden „viel zu viel Ermessensspielraum“ lasse. Einen Richtervorbehalt solle es zudem nicht geben. Eine schriftliche Anordnung der Staatsanwaltschaft reiche dem Entwurf nach aus, bei „Gefahr im Verzug“ dürfe diese sogar mündlich durch die Ermittlungspersonen ergehen. Die Polizei könne sich „also im Zweifel selbst dazu berechtigen“. Dies stehe in keinem Verhältnis zur Schwere des damit verknüpften Einschnitts in die Grundrechte.

• Mehr Online-Durchsuchungen und mehr

Mit dem Gesetzentwurf, der den Bundestag und den Bundesrat passieren muss, will die Regierung auch den Straftatenkatalog für heimliche Online-Durchsuchungen mit Staatstrojanern und den großen Lauschangriff in Paragraf 100b StPO „geringfügig“ ausdehnen und so „an die Bedürfnisse der Praxis“ anpassen. Aufgenommen werden sollen weitere Delikte aus dem Bereich des Menschenhandels und der Begleitdelikte, etwa der gewerbs- und bandenmäßige Computerbetrug sowie Tatbestände aus dem Außenwirtschafts- und dem Neue-psychoaktive-Stoffe-Gesetz. Die Zahl der heimlichen Online-Durchsuchungen werde so jährlich durchschnittlich, so die Gesetzesbegründung, von 12 auf 14 ansteigen, die der Wohnraumüberwachung von 8 auf 9. Das Kabinett will zugleich die klassische Telekommunikationsüberwachung bei bandenmäßiger Steuerhinterziehung in größerem Umfang als bisher ermöglichen.

Ermittler sollen künftig vor allem auf elektronische Beweismittel wie beim Provider gespeicherte E-Mails oder Chats, Inhalte eines Nutzerkontos eines sozialen Netzwerks sowie Daten in der Cloud auch heimlich zugreifen dürfen. Mit einem neuen § 95a soll es ihnen möglich werden die Bekanntgabe einer Beschlagnahme in bestimmten Konstellationen bei Straftaten von erheblicher Bedeutung und unter Beachtung des Verhältnismäßigkeitsgebots per gerichtlicher Anordnung zurückzustellen. Derlei Ausnahmen zu dem prinzipiell fortbestehenden Grundsatz der Offenheit solcher Zugriffe soll Fällen vorbehalten sein, „bei denen sich der zu beschlagnahmende Beweisgegenstand im Gewahrsam einer unverdächtigen Person befindet“. Werde offen beschlagnahmt, bestehe die Gefahr der Aufdeckung oder der Vereitelung des Ermittlungserfolgs, wenn eine gleichzeitig durchgeführte heimliche Strafverfolgung ihren Sinn verliere. Es gehe vor allem um Kinderpornographie, Handel mit Waffen, Drogen, Hehlerware und sonstigen verbotenen Gegenständen sowohl im Internet als auch im Darknet. Etwa auch bei Staatsschutzdelikten und Cyberkriminalität stünden die Fahnder hier immer wieder vor Herausforderungen.

Das Kabinett will auch die Regeln zur Postbeschlagnahme verschärfen. Ermittler sollen künftig auch Auskunft von Postdienstleistern über Postsendungen von oder an beschuldigte Personen verlangen können, die bereits ausgeliefert sind oder sich noch nicht beim Serviceanbieter befinden. Dies sei wichtig, „um eine effektive Strafverfolgung auch in Zeiten des vermehrten Online-Versandhandels zu gewährleisten“. Gerade der zunehmende Versand krimineller Ware „über das besonders abgeschottete Darknet“ könne mit dieser Handhabe besser aufgeklärt werden (Krempl, Bundesregierung: Kfz-Kennzeichen-Scanning kommt bundesweit, www.heise.de 20.01.2021, Kurzlink: https://heise.de/-5031140; Krempl, Bürgerrechtler warnen vor bundesweitem Kfz-Kennzeichen-Scanning, www.heise.de 23.01.2021, Kurzlink: https://heise.de/-5033739, vgl. DANA 4/2020, 245 f.; zur Ausweitung der strafrechtlichen Ermittlungsmöglichkeiten siehe auch die folgende Meldung).

Bund

Gesetzentwurf gegen Cybercrime-Plattformen

Gemäß einem Referentenentwurf aus dem Haus von Bundesjustizministerin Christine Lambrecht soll schärfer gegen den Verkauf etwa von Betäubungsmitteln, Waffen, Falschgeld, Darstellungen sexuellen Kindesmissbrauchs, gefälsch-

ten Ausweisen und gestohlenen Kreditkartendaten auf kriminellen Handelsplattformen im Internet vorgegangen werden können. Wer kriminelle Handelsplattformen gewerbsmäßig über das Darknet betreibt, soll laut dem Plan mit bis zu zehn Jahren Haft bestraft werden. Für weniger schwere Fälle sind eine Freiheitsstrafe von bis zu fünf Jahren oder Geldstrafe vorgesehen. Der Referentenentwurf aus dem Justizressort wurde von netzpolitik.org veröffentlicht. Ein neuer § 127 Strafgesetzbuch (StGB) richtet sich gegen Betreiber von Handelsplattformen, die den Zweck haben, Verbrechen sowie bestimmte Vergehen „zu ermöglichen oder zu fördern".

Die Straftaten, die erfasst werden sollen, sind in einem breiten Katalog aufgeführt. Dieser reicht von schweren Straftaten wie dem Inverkehrbringen von Falschgeld, dem Vorbereiten der Fälschung von Geld, Wertzeichen oder Zahlungskarten über den schweren sexuellen Missbrauch von Kindern und das Verbreiten, Erwerb oder Besitz verbotener Pornografie bis zu diversen Drogendelikten. Dazu kommen Verstöße gegen das Waffen- und Sprengstoffgesetz, aber auch gegen das Marken- und Designgesetz.

Laut der Begründung sollen ferner Vergehen eingeschlossen sein, „die häufig als Auftragstaten im Internet bestellt werden (´Crime-as-a-Service´)". Dabei könne es sich etwa um das Ausspähen oder Abfangen von Daten handeln. Aufgezählt wird schier die ganze Latte von Hackerparagrafen, die sich unter anderem auch gegen das Hehlen mit oder das Verändern von Daten sowie Computersabotage und -betrug richten. Das Ansetzen der Höchststrafe von mehr als fünf Jahren Freiheitsentzug sei denjenigen Delikten vorbehalten, „die ein besonders schweres Tatunrecht aufweisen und damit den Bereich der mittleren Kriminalität eindeutig verlassen". Um die angeführten Straftaten aufklären zu können, „sollen zugleich effektive Ermittlungsmöglichkeiten" dazukommen: „Die Strafverfolgungsbehörden müssen die Möglichkeit haben diesem Phänomen konsequent und effektiv zu begegnen."

Bei gewerbsmäßigem Handeln sollen die Fahnder die Telekommunikation Verdächtiger sowie genutzte Server überwachen und Staatstrojaner für heimliche Online-Durchsuchungen einsetzen können. Letzteres dürfen Ordnungshüter bislang allein im Kampf gegen „besonders schwere Straftaten". Der neue § 127 StGB soll im § 100b der Strafprozessordnung (StPO) aufgeführt werden, was der Polizei die Option eröffnet einen großen Lauschangriff nach § 100c StPO durchzuführen. Das Ministerium streift diesen Aspekt, mit dem die Ermittler ein besonders scharfes Schwert in die Hand bekommen sollen: Der Anwendungsbereich der akustischen Wohnraumüberwachung werde entsprechend „erweitert". Dies sei der Grund dafür, dass nicht nur in das Fernmeldegeheimnis, sondern auch in das Grundrecht auf Unverletzlichkeit der Wohnung eingegriffen werde.

Ausführlicher wirbt das Ressort für die Online-Durchsuchung, die als polizeiliches Instrument kaum weniger umstritten ist. Damit könnten „wichtige Erkenntnisse über weitere Tatverdächtige und über den Umfang der Straftat gewonnen werden, die auf anderem Wege nicht zu erlangen" seien. Der damit verbundene Eingriff in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sei „verhältnismäßig". Insgesamt würden die Befugnisse der Strafverfolger „moderat" ausgedehnt.

Auf Plattformen, „deren Zugang und Erreichbarkeit durch besondere technische Vorkehrungen beschränkt ist" und die etwa „im sogenannten Darknet betrieben werden", will das Ministerium nicht allein abstellen. Zwar böten solche Bereiche des Internets aufgrund „ihres hohen Maßes an Anonymität neben vielen rechtmäßigen und wünschenswerten Nutzungsmöglichkeiten auch eine optimale Umgebung für das Betreiben krimineller Handelsplattformen". Auch im offenen Teil des Internets gebe es aber „digitale Marktplätze, auf denen illegale Waren und Dienstleistungen gehandelt werden".

Zuvor hatten der Bundesrat und Bundesinnenminister Horst Seehofer (CSU) Gesetzesentwürfe vorgelegt, mit denen sie einen neuen Straftatbestand allein für das Betreiben illegaler Darknet-Handelsplätze schaffen wollten. Kritiker brachten dagegen vor, dass damit auch legitime „internetbasierte Leistungen" wie der Anonymisierungsdienst Tor kriminalisiert werden könnten. Im Koalitionsvertrag hatte Schwarz-Rot festgehalten: „Wo Strafbarkeitslücken bestehen, werden wir eine Strafbarkeit für das Betreiben krimineller Infrastrukturen einführen." Damit soll speziell im Internet eine Ahndung von Delikten wie das Betreiben eines Darknet-Handelsplatzes für kriminelle Waren und Dienstleistungen möglich werden. Diese Lücke besteht gemäß dem Referentenentwurf. Es gebe zwar schon spezialgesetzliche Verbote für den Verkauf bestimmter Waren und die Vorschrift zur Beihilfe im StGB. In den Fällen, in denen eine Verkaufsplattform aber vollautomatisiert betrieben werde, könne auf diesem Weg „allerdings nicht jeder Sachverhalt erfasst werden". Eine Kenntnis der Haupttat sei damit nämlich nicht immer gegeben, die Betreiber könnten so alles abstreiten.

Die Justizministerin Lambrecht sieht dringenden Handlungsbedarf. Die Anzahl krimineller Handelsplattformen nehme zu und es könne „nicht hingenommen werden", dass ihre Betreiber „sich nicht strafbar machen oder zumindest eine effektive Strafverfolgung nicht möglich ist". Bereits 2016 habe das BKA rund 50 entsprechende Plattformen gezählt. Es sei auch „eine deutliche Zunahme bei Angeboten von Hackertools und -dienstleistungen zu verzeichnen". Über die Portale würden massenhaft Straftaten ermöglicht und gefördert. Ein evtl. langwieriges Konsultationsverfahren mit der EU-Kommission sei daher „nicht angezeigt". Das Vorhaben sei mit der E-Commerce-Richtlinie vereinbar. Das Risiko, dass mit der Initiative legitime Online-Marktplätze wie eBay oder Amazon erfasst werden, sieht Lambrecht nicht. Vielmehr werde „Rechtssicherheit für Unternehmen gewährleistet, deren Geschäftsmodell das Betreiben von Plattformen mit rechtskonformen Angeboten ist". Manche Definition ist aber weit gestrickt. So werden etwa auch Foren einbezogen sowie nichtkommerzielle Aktivitäten wie „Tauschgeschäfte oder Schenkungen". Um auf Nummer sicher zu gehen, sollen „konkrete Umstände des Einzelfalls" geprüft werden (Krempl, Staatstrojaner und großer Lauschangriff gegen kriminelle Marktplätze, www.heise.de 26.11.2020, Kurzlink: https://heise.de/-4971297).

Bund

Bestandsdatenauskunft soll neu geregelt werden

Mit einem „Reparaturgesetz“ will das Bundesinnenministerium (BMI) die Regeln zur Bestandsdatenauskunft von Telekommunikations- (TK-) und Mediendiensten an Vorgaben des Bundesverfassungsgerichts (BVerfG) anpassen und zugleich ausweiten. Im Mai 2020 hatte das BVerfG geurteilt, dass der staatliche Zugriff auf Bestandsdaten wie Name, Anschrift und E-Mail-Adressen von Nutzern begrenzt werden muss (DANA 3/2020, 208 ff.). Mit einem vom BMI vorgelegten Entwurf sollen nicht nur die Übermittlungsvorschriften für die Dienstanbieter und die Abrufbestimmungen für Sicherheitsbehörden konkretisiert, sondern zugleich die Befugnisse insbesondere der Bundespolizei und von Zollfahndern ausweitet werden.

Das Vorhaben wird als eilbedürftig eingestuft, da aufgrund der Ansage des BVerfG auch der umstrittene Gesetzentwurf zur „Bekämpfung von Rechtsextremismus und Hasskriminalität“ auf Eis liegt. Bundespräsident Frank-Walter Steinmeier (SPD) hatte sich Anfang Oktober 2020 geweigert, die vom Bundestag zuvor im Juni beschlossene Initiative zu unterzeichnen, weil gemäß dem Urteil des BVerfG „eine hinreichend präzise Umgrenzung des Verwendungszwecks“ von Bestandsdaten nicht gewährleistet war. Gemäß dem „Anti-Hass-Gesetz“ müssen Anbieter von Telemediendiensten wie WhatsApp, eBay, Facebook, Google mit Gmail und YouTube, Tinder & Co. sensible Daten von Verdächtigen wie IP-Adressen und – in der Regel verschlüsselt gespeicherte – Passwörter künftig an Sicherheitsbehörden herausgeben. Der Gesetzgeber will damit die Möglichkeiten zur Bestandsdatenauskunft ausdehnen.

Das Bundeskriminalamt (BKA) sowie andere Strafverfolgungsbehörden und Geheimdienste könnten so etwa Kennungen, mit denen der Zugriff auf Nutzerkonten, Endgeräte und auf davon räumlich getrennte Speichereinrichtungen etwa in der Cloud geschützt wird, beispielsweise von sozialen Medien, Chatdiensten, Spiele-Apps, Suchmaschinen, Shops und privaten Seiten im Web, Webmail-Diensten, Podcasts und Flirt-Communities abfragen.

Das BMI will diesen breiten Zugang zu Bestandsdaten mit seinem Referentenentwurf für das „Reparaturgesetz“ auch der Bundespolizei sowie dem Zollkriminalamt und den Zollfahndungsämtern eröffnen. Deren Ermittler dürften die begehrten Informationen bislang nur bei TK-Anbietern erheben; bei Betreibern von Telemedien fehlt, so das BMI, eine „explizite Befugnisnorm“. Diese Lücke soll „unter gleichzeitiger Anpassung an die Vorgaben des Bundesverfassungsgerichts durch die Neufassung geschlossen“ werden.

Zu den künftig betroffenen Unternehmen zählen gemäß dem Entwurf „insbesondere Internetauktionshäuser oder -tauschbörsen, Anbieter von Videos auf Abruf oder Suchmaschinen im Internet“. Die Kommunikation verlagere sich zunehmend in soziale Netzwerke und Internetforen, wo eine Vielzahl von Mitgliedern einer Gruppe gleichzeitig informiert werden könne. Diese Möglichkeit werde auch dazu genutzt „Straftaten im Vorfeld konspirativ zu organisieren und zu lenken“.

Dazu gehörten im Zuständigkeitsbereich der Bundespolizei etwa „Verabredungen im Internet zu Gewalt gegen Bahnpersonal oder zu Anschlägen im Bereich von Bahnhöfen oder Flughäfen“. Mit den bisher den Ordnungshütern zur Verfügung stehenden Mitteln sei „eine adäquate Reaktion auf Straftaten, die auf diese Weise vorbereitet werden, nicht möglich“. Die „wachsende Bedeutung dieser Diensteanbieter bei der Aufklärung von Sachverhalten zur Gefahrenabwehr sowie der Verhütung und Verfolgung von Straftaten“ müsse sich daher auch im Instrumentarium der Bundespolizei widerspiegeln. Dies gelte analog für den Zoll.

Um den Auflagen des BVerfG nachzukommen, soll die Bundespolizei ein Ersuchen nach Bestandsdaten nur verlangen dürfen, um im Einzelfall eine Gefahr für die öffentliche Sicherheit oder Ordnung oder eine drohende Gefahr für ein Rechtsgut von erheblichem oder besonders schwerem Gewicht abzuwehren. Weitere Voraussetzung ist, dass „Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen“.

Der Entwurf will die Befugnisse der Diensteanbieter zur Weitergabe von Bestandsdaten nach dem Telekommunikationsgesetz (TKG) und dem Telemediengesetz (TMG) einander anpassen. Parallel sollen die korrespondierenden Abrufkompetenzen nach der „Doppeltürrechtsprechung“ auch für das BKA sowie alle drei Geheimdienste geändert werden. Die Reform der Landespolizeigesetze liegt in der Verantwortung der Länder.

In einem Begleitbrief des BMI heißt es: „Die Übermittlungs- und Erhebungszwecke werden dem Bestimmtheitsgebot entsprechend normenklar geregelt.“ Dazu gehöre auch, dass die Weitergabe der Daten an das BKA und Zollkriminalamt in deren Zentralstellenfunktion als Drehscheibe für andere Strafverfolgungsbehörden ausdrücklich geregelt werde. Dem Grundsatz der Verhältnismäßigkeit folgend würden die Eingriffsvoraussetzungen abgestuft: „Je weiter die Befugnisausübung im Vorfeld einer konkreten Gefahr ermöglicht wird, desto gewichtiger muss das zu schützende Rechtsgut oder desto schwerer die zu verhütende Straftat sein.“ Ferner würden bislang zwar schon praktizierte, aber gesetzlich noch nicht vorgesehene behördliche Dokumentationspflichten festgeschrieben.

In den einzelnen Gesetzen für die Sicherheitsbehörden des Bundes will das BMI so etwa klarstellen, dass „die Auskunft nur verlangt werden“ dürfe, „wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen“. Teils reichen die Kompetenzen aber nach wie vor recht weit. Das BKA etwa soll auch Bestandsdaten abfragen dürfen, um „Auskunftsersuchen einer ausländischen Strafverfolgungsbehörde im Rahmen des polizeilichen Dienstverkehrs“ zu erledigen. Die Befugnis gelte ferner, wenn „die konkrete Gefahr besteht, dass eine Person an der Begehung“ einer schweren Straftat „beteiligt sein wird“. Der Verdacht könne dabei auch durch eine „konkrete Wahrscheinlichkeit“ begründet werden. Das Bundesamt für Verfassungsschutz soll zudem „Zugangssicherungsinformationen“ wie PIN und PUK nicht mehr nur bei TK-Unternehmen, sondern, was neu

wäre, auch bei Telemediendiensten erfragen dürfen.

Die im Anti-Hass-Gesetz vorgesehene breite Klausel zur Herausgabe von Passwörtern kann laut der Begründung unverändert bleiben. Sie entspreche den BVerfG-Anforderungen. Juristen sehen die Pflicht zur Weitergabe strafrechtlich relevanter Inhalte inklusive IP-Adressen und Portnummern durch Facebook & Co. ans BKA als kritisch an, da diese sich zunächst auf reine Verdachtsfälle bezieht. Die Grünen fordern hier ein zweistufiges Verfahren. Das BMI hat diesen Ansatz nicht aufgegriffen.

Verbände hatten insgesamt nur eine Woche Zeit, den gleichzeitig mit den anderen Ressorts abzustimmenden Entwurf zu kommentieren. Im Rekordtempo sollte das Vorhaben noch vor Weihnachten durch den Bundestag und den Bundesrat geschleust werden. Nicht haltbare Bestimmungen aus dem gestoppten Anti-Hass-Gesetz werden dem Plan nach aufgehoben, die überarbeiteten einschlägigen Artikel „erneut eingebracht".

Grünen-Fraktionsvize Konstantin von Notz hielt es für zweifelhaft, dass das Verfahren so durchgezogen werden kann. Dass das vorgesehene Gesetz diesmal höchstrichterlichen Vorgaben gerecht werde, sei fraglich. Auf jeden Fall komme auf das BKA mit der Meldepflicht durch Betreiber sozialer Netzwerke eine „Denial-of-Service-Attacke" zu. Das ganze Vorgehen der Bundesregierung habe das Potenzial, „den wichtigen Kampf gegen Rechtsextremismus und strafbare Meinungsäußerungen im Internet zu erschweren" (Krempl, Bestandsdaten: Bundespolizei und Zoll sollen auf Passwörter zugreifen dürfen, www.heise.de 28.11.2020, Kurzlink: https://heise.de/-4973625; Hängepartie beim Gesetz zur Bekämpfung des Rechtsextremismus hält an, www.gruene-bundestag.de 16.12.2020).

Bund

BND-Kontrollgesetz weiterhin streitig

Das Bundeskanzleramt legte Ende November 2020 die Überarbeitung eines Gesetzentwurfs vor, wonach der Bundesnachrichtendienst (BND) Journalisten nur noch in Ausnahmen belauschen darf, und reagiert damit auf umfangreiche Proteste und eine Verfassungsbeschwerde. Beim weltweiten Telefoneanzapfen oder Mitlesen von E-Mails soll der BND künftig mehr Respekt vor ausländischen Journalistinnen und Journalisten zeigen.

Journalisten hatten darauf hingewiesen, dass sie mit Informanten vertraulich sprechen können müssen, besonders wenn diese die Verfolgung durch ein ausländisches Regime fürchten. Journalistenverbände hatten daher eine Verfassungsbeschwerde gegen den BND angestrengt und mit Datum vom 18.05.2020 in einem umfangreichen Urteil des Bundesverfassungsgerichts (BVerfG) Recht bekommen (DANA 3/2020, 202 ff.).

Während es in einem ersten Gesetzentwurf aus dem Bundeskanzleramt vom September 2020 noch geheißen hatte, der BND solle ausländische Journalisten künftig immer dann abhören dürfen, wenn dadurch „Erkenntnisse" über „krisenhafte Entwicklungen im Ausland" gewonnen werden könnten (DANA 4/2020, 242 f.), hat sich die Regierung offenbar umstimmen lassen, so der Geschäftsführer von Reporter ohne Grenzen, Christian Mihr: „Die Hürden sind jetzt deutlich, deutlich höher". Das habe ihn überrascht. Offenbar hätten sich die Diskussionen in den vorangegangenen Wochen gelohnt.

Nach dem neuen, überarbeiteten Entwurf darf der BND ausländische Journalisten nur noch belauschen, wenn diese selbst Täter oder Teilnehmer bestimmter schwerer Straftaten sind. Oder wenn dies „notwendig ist zur Verhinderung einer Gefahr" für Leib oder Leben, lebenswichtige Güter oder den Bestand eines EU-Staats oder der Nato.

Kern der vom BVerfG eingeforderten Reform ist, dass in Deutschland ein völlig neues System der Kontrolle der BND-Abhörpraktiken geschaffen wird. Die Bundesregierung spricht im Gesetzentwurf von einem „Unabhängigen Kontrollrat" aus sechs erfahrenen Juristinnen und Juristen, die von Bundestagsabgeordneten gewählt werden sollen. In der ersten Fassung des Gesetzentwurfs vor zwei Monaten stand noch, dass der BND in Ausnahmefällen aus Gründen des „Staatswohls" Dinge vor diesem Kontrollrat geheim halten dürfe. Auch an diesem Punkt gibt die Bundesregierung nun der Kritik nach. Der künftige Kontrollrat soll alles einsehen dürfen.

Weiterhin soll die Einschränkung gelten, dass die Kontrolleure vor solchen IT-Systemen Halt machen müssen, die der BND mit ausländischen Geheimdiensten gemeinsam betreibt. Auch Gebäude, in denen der BND etwa mit dem US-Abhörgiganten NSA zusammenarbeitet, sollen die Mitglieder des Kontrollrats nicht betreten dürfen. Das könnte in der Praxis sehr wichtig werden. Der BND arbeitet in vielen Bereichen eng mit ausländischen Geheimdiensten zusammen, die sich eine Kontrolle durch eine von der Regierung unabhängige Instanz in Deutschland verbitten wollen. Dieser Bereich würde einer rechtsstaatlichen Kontrolle wohl unzugänglich bleiben.

Auch aus diesem Grund spricht der Vorsitzende der Gesellschaft für Freiheitsrechte, Ulf Buermeyer, der im Mai gemeinsam mit Reporter ohne Grenzen in Karlsruhe gegen den BND gesiegt hatte, von einer „Provokation": „Nach wie vor versucht die Bundesregierung, entgegen der Entscheidung des Bundesverfassungsgerichts vom Mai 2020 eine wirklich effektive und unabhängige Kontrolle des BND zu verhindern." Das Problem beschränkt sich nicht allein auf die Zusammenarbeit mit fremden Staaten. Auch wenn der BND mit inländischen Stellen wie etwa dem Bundeskriminalamt oder dem Verfassungsschutz kooperiert, soll dies dem Einblick durch die Kontrolleure entzogen bleiben.

Dies betrifft die sogenannten projektbezogenen gemeinsamen Dateien, die der BND etwa mit dem Bundeskriminalamt für je fünf Jahre gemeinsam führt und die er nach dem neuen Gesetzentwurf künftig auch mit der Bundeswehr gemeinsam führen soll. Der Gesetzentwurf aus dem Kanzleramt wurde am 16.12.2020 im Bundeskabinett beschlossen und soll im Frühjahr im Bundestag debattiert werden.

(Steinke, Abhören mit Auflagen, SZ 01.12.2020, 5; Meister, Bundesregierung beschließt Geheimdienst-Überwachung wie zu Snowden-Zeiten, netzpolitik.org 16.12.2020).

Bund

EGMR lässt Klage gegen BND zu

Der Europäische Gerichtshof für Menschenrechte (EGMR) in Straßburg hat eine Beschwerde gegen den Bundesnachrichtendienst (BND) zur Entscheidung angenommen. Es geht um den Verdacht, dass der BND millionenfach E-Mails von Deutschen durchleuchtet hat. Es geht dabei auch um die Frage, ob Bürger gegen Maßnahmen Rechtsschutz erlangen können, die derart geheim gehalten werden, dass sie nicht einschätzen können, ob sie davon betroffen sind.

In der jüngeren Zeit sind einige Urteile ergangen, die den BND in seiner jahrelangen Abgeschiedenheit gestört haben. 2017 äußerte das Bundesverwaltungsgericht (BVerwG) Einwände gegen die Massenüberwachung des BND und die Speicherung von Verbindungsdaten von Telefongesprächen in der Datenbank „Veras". Die Richterinnen und Richter sahen dafür keine Rechtsgrundlage (DANA 1/2018, 54 f.). Inzwischen hat der Bundestag eine Rechtsgrundlage geschaffen, die Speicherung von Verkehrsdaten für sechs Monate ist dem BND jetzt ausdrücklich erlaubt.

Mai 2020 ließ das Bundesverfassungsgericht ein mehr als 300 Seiten dickes Urteil folgen, in dem das höchste deutsche Gericht das Überwachen von Ausländern im Ausland durch den BND begrenzt (DANA 3/2020, 202 ff.). Die Grundrechte des Grundgesetzes seien auch dort stets zu beachten. Ausländer seien kein „Freiwild" für die deutschen Überwacher. Die Bindung an das Grundgesetz gelte, was die Bundesregierung jahrelang bestritt, auch für die Lauscher und Hacker hinter dem BND-Zaun.

Nun sind die Chancen gestiegen, dass die Justiz als nächstes auch die Rechte von Inländern gegenüber dem Geheimdienst stärkt. Der EGMR hat eine Beschwerde der Journalistenorganisation „Reporter ohne Grenzen" gegen den BND zur Entscheidung angenommen. Nur sehr wenige Beschwerden nehmen bei dem Gerichtshof in Straßburg diese Hürde. Schon mit der Annahme zur Entscheidung ist eine bemerkenswerte Botschaft des europäischen Gerichts verbunden: Die deutsche Justiz ist immer noch zu zurückhaltend gegenüber den eigenen Geheimdiensten.

In dem Fall geht es wieder um die Massenüberwachung durch den BND. Für den Geheimdienst ist diese alltägliche Routine. Der Dienst durchsucht die Kommunikation über das Internet, schaltet sich vor allem an großen Internetknotenpunkten wie in Frankfurt am Main in Leitungen ein und filtert dann den Datenstrom nach bestimmten Begriffen, die auf politisch Brisantes hindeuten könnten. Tausende „Treffer" pro Tag erzielt der Dienst auf diese Weise. Sie werden anschließend von Agenten gelesen und analysiert.

Eigentlich sollten deutsche Bürger vor einer solchen BND-Überwachung ihrer E-Mails und Chats geschützt sein. Der Geheimdienst verwendet deshalb verschiedene technische Mittel, um die Nachrichten vorab herauszufischen. Das ist aber denkbar schwierig. Deutsche schreiben ihre E-Mails nicht nur von Domains, die auf .de enden, sie telefonieren auch nicht nur von Anschlüssen, die eine deutsche Vorwahl haben. Unabhängige Technikfachleute waren noch nie recht überzeugt von den Beteuerungen des BND, dass man zu einer sauberen Trennung hier wirklich in der Lage sei. Ihr Verdacht besteht darin, dass auch E-Mails von Deutschen durchleuchtet und teils gelesen werden.

2013 hatte sich deshalb „Reporter ohne Grenzen", vertreten durch den Datenschutzanwalt Niko Härting, hilfesuchend an das BVerwG in Leipzig gewandt. Es war das Jahr der Enthüllungen von Edward Snowden. Der amerikanische Whistleblower hatte der Welt gerade vor Augen geführt, wie sehr die weltweite Massenüberwachung seit den Anschlägen vom 11.09.2001 zugenommen hatte.

Doch bei dem BVerwG, das in erster Instanz für Klagen gegen den BND zuständig ist, wurden die Kläger mit diesem Anliegen abgewiesen (DANA 1/2017, 64 f.). Die Richter wollten sich mit der Beschwerde nicht einmal beschäftigen. Und auch beim höchsten deutschen Gericht, dem Bundesverfassungsgericht, an das sich die Kläger als nächstes wandten, lief es 2017 nicht anders. Die Richter erklärten: Nur wer nachweisen könne, dass er oder sie vom BND überwacht worden sei, dürfe klagen. Das heißt dann in der Praxis: so gut wie niemand. Diese Haltung der Justiz schützt den BND.

So kommt nun der EGMR ins Spiel. Der Gerichtshof hat sich am 09.12.2020 an die Bundesregierung gewendet und juristisch-nüchtern die Frage nach „wirksamen Rechtsbehelfen" gegen derartige Geheimoperationen gestellt (Az. 81993/17). Der Kläger hatte in seiner Beschwerdeschrift moniert, dass er den Beweis, heimlich überwacht worden zu sein, „aufgrund der Heimlichkeit der Maßnahmen und der umfassenden Löschung der erfassten Nachrichten nicht führen" kann. Für den Geschäftsführer von „Reporter ohne Grenzen" Christian Mihr ist deshalb die bisherige Haltung der deutschen Gerichte „absurd".

Der Straßburger Gerichtshof ist zuständig für alle 47 Staaten, die der Europäischen Menschenrechtskonvention (EMRK) angehören. Sollte er am Ende urteilen, dass es in Deutschland einfacher werden muss den BND zu verklagen, wäre dies zwar nicht bindend. Andere Staaten wie etwa Russland oder die Türkei ignorieren Urteile des EGMR regelmäßig. Allerdings hat sich die Bundesrepublik in der Vergangenheit stets dem Straßburger Votum gebeugt, zuletzt hat sie deshalb etwa das System der Sicherungsverwahrung im Strafvollzug neu geordnet. Bis März 2021 hat die Bundesregierung Zeit, eine Stellungnahme in dem Verfahren abzugeben. Mit einer Entscheidung des Gerichtshofs wird nicht vor 2022 gerechnet (Steinke, Klage gegen Bundesnachrichtendienst zugelassen, www.sueddeutsche.de 11.01.2021; Dämpfer für die Lauscher, SZ 11.01.2021, 6).

Bund

BMJ gegen Scheuers KFZ-Daten-Regelungsvorschläge

Das Bundesjustizministerium (BMJ) monierte in mehreren Punkten ein geplantes Gesetz des Bundesverkehrsministeriums von Andreas Scheuer (CSU) für automatisiertes Fahren, u.a. weil Daten künftig an Verfassungsschutz und Bundeskriminalamt übermittelt werden

sollen. Das BMJ verweigerte unter anderem aus diesem Grund, dem Entwurf zuzustimmen. Das BMJ fordert vom Verkehrsministerium, die entsprechenden Vorschriften in dem Gesetz- und im Verordnungsentwurf „zu streichen“: Bei den Daten, die erhoben würden, handele es sich auch um „sensible personenbezogene Datenkategorien, die beim autonomen Fahren anfallen, wie etwa die Positionsdaten des Fahrzeugs, aus denen sich Bewegungsprofile der Fahrzeuginsassen erstellen lassen würden“.

Da es keinen Schutz dieser Daten gebe, widerspreche das den Anforderungen, die das Bundesverfassungsgericht dem Gesetzgeber aufgegeben habe. „Auch die Begründung lässt nicht erkennen, ob eine Übermittlung der genannten Daten zur Erreichung eines legitimen Regelungszwecks geeignet, erforderlich und angemessen erscheint.“

Der hochsensible Bereich der personenbezogenen Daten ist nur ein Kritikpunkt an dem Plan von Minister Scheuer. Dieser will noch in dieser Legislaturperiode das Gesetz durch den Bundestag bringen, mit dem die Automobilhersteller autonom fahrende Fahrzeuge im regulären Straßenverkehr einsetzen können. Zunächst soll dies im Nahverkehr durch Kleinbusse, sogenannte „People Mover“, möglich sein.

Bereits in einer ersten Stellungnahme hatten die Beamten von Justizministerin Christine Lambrecht (SPD) grundlegende Bedenken geäußert. Das Verkehrsministerium reagierte darauf Mitte Dezember 2020, offenkundig aber wenig überzeugend, wie sich aus der 19 Seiten umfassenden zweiten Replik ergibt. Darin legen die Beamten sogar einen eigenen Entwurf für ein Mobilitätsdatengesetz vor und lassen kein gutes Haar an den Plänen von Minister Scheuer: „Die Entwürfe für ein Gesetz und für eine Verordnung zum autonomen Fahren sind aus hiesiger Sicht weiterhin inhaltlich, rechtsförmlich und rechtssystematisch anpassungsbedürftig.“

Sie seien „erkennbar noch nicht aus einem Guss“. Angesichts der zahlreichen Defizite sei eine „nochmalige Vorlage von wesentlich überarbeiteten Entwürfen“ seitens des Bundesverkehrsministeriums erforderlich. Auch verweist das Justizressort „auf die Notwendigkeit, für die abschließende Rechts- und Mitprüfung angemessene Fristen einzuräumen“. Mit dem Hinweis gilt innerhalb der Bundesregierung als so gut wie sicher, dass das Gesetz in dieser Legislaturperiode nicht mehr umgesetzt werden kann.

Dabei schließt sich das BMJ grundlegend der Meinung an, dass autonome Fahrzeuge vor allem im Nahverkehr „maßgeblich dazu beitragen“ können, dass etwa ältere und behinderte Menschen „im urbanen, aber vor allem auch im ländlichen Raum“ deutlich mobiler sind. Auch ein Beitrag zum Klimaschutz werde damit geleistet. Notwendig sei aber „ein ausgewogener Rechtsrahmen“. Die Pläne des Verkehrsministers trügen allenfalls dem „Innovationsdrang der Technologie“ Rechnung, so auch das Vorblatt des Gesetzentwurfes.

Das Justizressort plädiert „hinsichtlich der Mobilitätsdaten für eine Regelung zur Datensouveränität, für Regelungen zur Datenverarbeitung, zum erlaubten Zugriff auf die Fahrzeugdaten, für eine nutzerfreundliche Software im KFZ und für eine Regelung zur Bereitstellung von Fahrzeugdaten für Gemeinwohlzwecke“ – und macht dafür konkrete Vorschläge. Der Kern, der ins Straßenverkehrsgesetz eingefügt werden soll: Der Halter des Fahrzeugs oder „die Person, die das Fahrzeug dauerhaft nutzt“, ist Herr „aller Daten“. Gemeint ist „jegliche Datenverarbeitung, insbesondere das Generieren, Erheben, Erfassen und Speichern sowohl von personenbezogenen Daten als auch von technischen Daten ohne Personenbezug“. Alles andere sei ein Verstoß gegen die Datenschutz-Grundverordnung der Europäischen Union.

Der Halter muss aus Sicht des Ministeriums die „Datensouveränität“ besitzen. Das gelte auch für Daten, die etwa der Hersteller erhebt, um den Verschleiß von Fahrzeugteilen zu ermitteln. Entsprechend dürften Volkswagen, Daimler, BMW oder Toyota in ihren Allgemeinen Geschäftsbedingungen nicht festlegen, dass der Halter auf seine Datenhoheit verzichtet, wenn er das Fahrzeug kauft. Auch müsse der Hersteller ermöglichen, dass der Halter Daten selbst speichert und über offene Schnittstellen etwa an einen „Datentreuhänder“ übermittelt. Damit wird ein Datenmonopol der Autohersteller unterbunden.

Einige Daten aber will auch das Justizministerium gern nutzen: Daten, die keine Rückschlüsse auf die Person erlauben, sollen auch der Allgemeinheit zur Verfügung stehen können. Sie sollen an eine „zentrale Anlaufstelle“ übermittelt und etwa zur Verkehrs- und Stadtplanung genutzt werden (Delhaes, Mangelnder Datenschutz: Justizministerin lehnt Scheuers Gesetz zum autonomen Fahren ab, www.handelsblatt.com 19.01.2021).

Bund

Kartellamt: Datenschutzverstöße beim Smart-TV

„Smart-TVs“ sind aus den Wohnzimmern kaum noch wegzudenken. Mit ihrer Anbindung an das Internet und über diverse Apps bieten sie die Möglichkeit, Streamingdienste ebenso zu nutzen wie Mediatheken oder Video-Plattformen. Viele smarte Fernseher sammeln Daten, ohne die Nutzer zu informieren. Oder die Bestimmungen dazu sind so undurchsichtig, dass sich viele in ihr Schicksal ergeben. Über den „Roten Knopf“ wird die HbbTV-Funktion für den Abruf von Zusatzinfos oder Nachrichten aktiviert. Hybrid Broadcast Broadband TV (HbbTV) ermöglicht es, Internetinhalte mit dem Fernsehbild zu verbinden. Wegen ihrer ständigen Anbindung ans Internet sind Smart-TVs quasi prädestiniert Nutzungsdaten zu sammeln, weiterzugeben und sie gegebenenfalls sogar für personalisierte Werbung einzusetzen.

Gemäß einer Untersuchung des Bundeskartellamts können „das generelle Fernsehverhalten einer Person, ihre App-Nutzung, ihr Surf- und Klickverhalten oder auch biometrische Daten wie Stimme oder Cursorbewegungen sowie die im Einzelnen über den Fernseher abgespielten Inhalte erfasst und ausgewertet werden.“

Viele TVs haben Google Assistant, Alexa oder Siri integriert oder sind damit kompatibel. Dadurch lassen sich die Fernseher und andere Smart-Home-Geräte per Sprache steuern. Zudem können die Hersteller unter anderem Standort und IP-Adresse übertragen, die beispielsweise an Netflix und dritte Werbeanbieter geleitet werden, unab-

hängig davon, ob man ein Konto bei dem Streaminganbieter hat oder nicht. Darüber hinaus könnten etwa Gerätetyp und Ort sowie die TV-Seriennummer und der Name des WLAN-Netzwerks erfasst werden, womit theoretisch ein Nutzerprofil erstellt werden kann.

Nach Angaben von Ulrike Kuhlmann von c´t werden bereits bei der Installation einiger Smart-TVs über 60 Server angesprochen, etwa von Google, Amazon und Microsoft: „Nutzen Sie die HbbTV-Funktion, lässt sich jeder Klick mit der Fernbedienung nachverfolgen." Sie empfiehlt, den „Roten Knopf" einfach zu deaktivieren, wenn man ihn sowieso nicht nutzt.

Wie intensiv Daten gesammelt werden, ist abhängig vom Hersteller, wobei in der Regel günstigere TV-Geräte mehr Daten sammeln als die im höherpreisigen Segment. Nutzer können zumeist nicht erkennen, welche Daten gesammelt werden. Nach Angaben des Bundeskartellamts wiesen die Datenschutzbestimmungen der untersuchten Hersteller „schwerwiegende Transparenzmängel" auf. Die Datenschutzbestimmungen seien vor allem deshalb für Verbraucher nicht nachvollziehbar, weil sie für eine Vielzahl von Diensten und Nutzungsprozessen gelten sollen. Sich vor einem Kauf über den Datenschutz des Anbieters zu informieren – etwa über dessen Website – sei praktisch unmöglich.

Teils kann man der Sammelei und Verwendung von Daten widersprechen, am besten gleich bei der Ersteinrichtung des Geräts. Dazu Kuhlmann: „Das hat keinen Einfluss auf die anderen Funktionen, auch wenn das von den Herstellern suggeriert wird." Sollte später ein Dienst tatsächlich nicht funktionieren, ließe sich der Datenzugriff im Nachhinein wieder über die Einstellungen erlauben. Eine weitere Option besteht Kuhlmann zufolge darin eine Blacklist im Router anzulegen, dann darf der Fernseher nur bestimmte Server ansteuern. Das sei jedoch recht aufwändig und eher für Versierte und Spezialisten geeignet: „Es gibt zwar vorgefertigte Listen, die muss man aber permanent pflegen."

Simone Warnke vom Onlinemagazin „Inside-digital.de" gibt den Rat, Apps, die man auf dem Fernseher gar nicht nutzt, zu deinstallieren, inklusive Anwendungen für Sprachsteuerung oder Kameras, falls vorhanden. Jede App, insbesondere wenn sie nicht aktualisiert wird, sei ein zusätzliches Sicherheits- und Datenschutz-Risiko.

Bei etlichen Herstellern ist laut Bundeskartellamt nicht gesichert, dass der Sicherheitsstandard der Geräte in den Jahren nach dem Kauf durch Software-Aktualisierungen aufrechterhalten wird. Kein Unternehmen mache verbindliche Angaben dazu, wie lange es seine Produkte mit Sicherheitsupdates versorgt. Andreas Floemer vom Digitalmagazin t3n erläutert: „Bei fehlenden Sicherheitsupdates ist die Wahrscheinlichkeit größer, dass kriminelle Hacker sich Zugriff auf den Fernseher verschaffen können, um etwa per Webcam oder Mikrofon zu sehen und zu lauschen, was beim Nutzer im Wohnzimmer passiert". Auch Zugangsdaten zu verknüpften Diensten könnten ausgespäht werden.

Zum Schutz vor Hackern rät Kuhlmann, den Fernseher zuhause nur mit dem Gäste-WLAN zu verbinden. So könne der Fernseher zumindest nicht mit den anderen Geräten im Netzwerk kommunizieren, wenngleich eine Datensammlung weiter möglich sei (Wenn der Fernseher Daten sammelt, www.fr.de 19.11.2020).

Bundesweit

Umfrage bei Autofahrern bestätigt deren Wunsch nach Selbstbestimmung

Gemäß einer von forsa durchgeführten repräsentativen bundesweiten Umfrage bei 1007 Autofahrern im Auftrag der Dekra möchte eine große Mehrheit (88%) der Autofahrer in Deutschland selbst bestimmen, was mit den Daten aus dem eigenen Fahrzeug geschieht. Derzeit gibt es noch keine gesetzliche Regelung, die die Nutzung der Kfz-Daten regelt, die u.a. Auskunft geben über Fahrzeugzustand oder Fahrstil der Fahrer. 38% meinten, das Recht auf Bestimmung der Datennutzung solle auch dem jeweiligen Fahrer zustehen, wenn er nicht Fahrzeugeigentümer ist, zum Beispiel bei Mietwagen.

Die große Mehrheit (72%) möchte nicht, dass andere – Werkstatt, Versicherung oder Behörden – erfahren, wie ihr Fahrstil ist. 63% finden es hingegen gut, wenn sie die Werkstatt oder der Hersteller durch den Zugriff auf Fahrzeugdaten auf nötige Reparaturen aufmerksam macht. 46% äußerten die Befürchtung, dass sie über den Datenzugriff von anderen ausgespäht werden: also dass ihr Fahrverhalten analysiert wird oder dass ihr Fahrzeug gehackt werden könnte und dadurch ihre Sicherheit beim Fahren gefährdet sein könnte.

80% erwarten, dass sich voll automatisierte Autos, die komplett eigenständig fahren, früher oder später durchsetzen werden. 42% rechnen damit, dass dies in den nächsten 10 bis 20 Jahren der Fall sein wird. 26% denken, dass es später soweit kommen wird. An das voll automatisierte Fahren in naher Zukunft (in weniger als zehn Jahren) glauben 12% der Befragten (PE DEKRA 15.01.2021, Mein Auto, meine Daten!).

Bundesweit

Kontodatenzugriff für die Schufa

• Der Test

Der Telefonanbieter Telefónica/O2 testete Ende 2020 eine Kooperation mit der Auskunftei Schufa und deren Tochter FinAPI. Das Angebot „Schufa Check Now" nimmt dabei Zugriff auf die Kontodaten der Verbraucher beim kontoführenden Finanzinstitut. Die Daten werden dann durchleuchtet und geprüft, ob die Finanzsituation des Betroffenen besser aussieht, als der Score vermuten lässt, um ihm so eine zweite Chance auf den Vertrag einräumen. Bei dem Verfahren sollten mögliche Neukunden, die aufgrund ihrer schlechten Bewertung normalerweise keinen Handyvertrag bekommen würden, sich von der Schufa auf ihr Konto schauen lassen: „Denn bei Telefónica gibt es vereinzelt potenzielle Kunden, deren Vertragswunsch aufgrund einer fehlenden beziehungsweise unzureichenden oder älteren negativen Bonitätsinformation abgelehnt werden musste, obwohl ihre aktuelle finanzielle Situation völlig unproblematisch war." Die Daten dazu werden nur für den Zweck und ganz kurz gespeichert, hieß es von Seiten der Schufa.

Das Angebot war nur ein kleiner Ausschnitt von größeren Pläne. Aus internen Dokumenten geht hervor, dass die Schufa mit ihrem Dienst das Ziel verfolgt, einen detailgetreuen Einblick in Millionen Kontoauszüge zu bekommen. Dieses Wissen hätte dann in eine Art Superscore einfließen können.

Wie die Schufa mit Sitz in Wiesbaden an die Daten gelangen möchte, zeigte der Test mit Telefónica: Auf der Webseite stand ein kleines Kästchen, das Verbraucher freiwillig anhaken können – ein Klick mit großen Auswirkungen: Mit ihm nämlich gibt der Kunde der Auskunftei die Erlaubnis, seine Kontoauszüge zu lesen, diese Daten für zwölf Monate zu speichern und daraus auch eigene Produkte zu entwickeln. Die Schufa betonte, dass man in der Testphase keine Daten speicherte. „Über die spätere Ausgestaltung des finalen Produktes können wir derzeit daher noch keine Auskunft geben."

Was ein Blick auf die höchstpersönlichen Kontodaten offenbaren kann, ist der Schufa sehr wohl bewusst. 2020 hielt der Vertriebsmanager der Tochterfirma FinAPI einen Vortrag vor einigen potenziellen Kunden. Auf einer Folie zeigte er zwölf Kategorien und 65 Unterkategorien, die man auslesen könnte. Dazu gehören beispielsweise das Gehalt, Unterhaltszahlungen, Ausgaben für Heimwerken und Garten, für Strom, für Gas, für Versicherungen oder für Wellness. Außerdem könne man sogenannte „Risikofaktoren" erkennen, beispielsweise Glücksspiel oder Zahlungen an Inkassoinstitute. Was die Schufa zwölf Monate lang mit diesen Daten machen will, wollte sie auf Anfrage nicht sagen.

• Erste Reaktionen

Datenschützer zeigten sich entsetzt. Peter Schaar, von 2003 bis 2013 Bundesdatenschutzbeauftragter, vermutete, dass niemand die „tatsächliche Reichweite dieser Einwilligung überschauen" kann. Dabei mache man sich mit der Erlaubnis „wirklich nackig". Er fürchtet, dass so umfassende Persönlichkeitsprofile entstehen – zum Nachteil der Verbraucher: „Wenn jemand sich an irgendwelchen Online-Wetten beteiligt, dann wird das sich sicherlich nicht positiv auf die Bonität auswirken". Der Kunde bekäme womöglich nicht nur keinen Handyvertrag, sondern „auch keinen Versicherungsvertrag oder keinen Kredit". Thilo Weichert, bis 2015 Datenschutzbeauftragter des Landes Schleswig-Holstein, fand das ebenfalls „hochproblematisch". Die hochsensiblen Daten würden hier ausschließlich im Unternehmensinteresse verwendet, ohne dass der Betroffene das nachvollziehen könne: „Das ist für mich tatsächlich ein Horror."

Klaus Müller, Vorstand des Verbraucherzentrale Bundesverbands, warf der Schufa „Kontoschnüffelei" vor. „Eine solch tiefe Datenauswertung der Kontobewegungen für Scoringzwecke erlaubt Rückschlüsse auf Persönlichkeit, wirtschaftlichen Status und selbst politische Orientierungen der Kunden und führt damit letztlich zum vollkommen durchleuchteten Verbraucher." Man prüfe rechtliche Schritte für den Fall, dass die Auskunftei diese Pläne umsetzt.

• Erweitertes Schufa-Geschäftsmodell

Die Pläne der Schufa gehen weit über das hinaus, was die Schufa bisher macht. Sie selbst sagt, dass sie weder das Einkommen noch das Vermögen der Menschen kenne. Mit dem Blick aufs Konto oder mithilfe der „Datenspende", die über das kleine anzuklickende Kästchen eingeholt werden könnte, würde sich das schlagartig ändern. Interne Unterlagen und Auftritte in den vergangenen Monaten lassen vermuten, was die Schufa seit Ende Dezember 2018 vorhat, indem sie FinAPI kaufte. Das Münchener Start-up bringt einen großen Vorteil mit sich: Es hat eine Lizenz der Finanzaufsicht Bafin fürs Lesen von Konten, was aufgrund der sog. europäischen PSD-2-Richtlinie rechtlich möglich ist. Bereits vor dem Zukauf, so zeigt es ein Dokument, spielte man mit dem Gedanken einer kontinuierlichen Kontoeinsicht sowie einer regelmäßigen Übertragung und Speicherung der Daten bei der Schufa zur „Berechnung von Scores bei jeder Anfrage".

In einer Präsentation von 2019 wird es konkreter. Dort listet die Schufa unter dem Punkt „aktuelle Produktentwicklungsansätze" einige Vorschläge auf: „Neue Scores, Ergänzung bestehender Scores um zusätzliche Indikatoren, zudem Kontoführungsscores, integrierte Scores, diverse Affinitätsscores". Dies bedeutet, dass die Schufa die Vorlieben der Verbraucher erkennen und bewerten könnte.

Fast zwei Jahre später, am 04.11.2020, ging das Projekt „Schufa Check Now" als Webseite online, inklusive des kleinen Kästchens zur freiwilligen Einwilligung in eine Datenspende. Während sich Schufa-Mitarbeiter einen Tag vor dem Pilotstart zumailten: „Drückt uns die Daumen, dass die Lösung fliegt", waren die zuständigen Landesdatenschützer in Bayern noch ahnungslos. Sie erfuhren von dem Test erst am Tag, nachdem die Seite online gegangen ist; das Bayerische Landesamt für Datenschutzaufsicht prüft nun den Sachverhalt. Der Leiter der Behörde, Michael Will, zeigte sich skeptisch, beispielsweise, ob diese Kombination der Firmen „so legitim, so hinnehmbar" sei. Seien es doch „zwei unterschiedliche Geschäftsmodelle, mit denen wir es hier zu tun haben".

Auf Anfrage teilte Telefónica/O2 zunächst mit, man teste „lediglich in einem Pilotprojekt" mit einer geringen Zahl von Nutzern die Akzeptanz für ein solches Verfahren. Die Teilnahme sei freiwillig. Datenschutzrechtlich verantwortlich sei die Schufa.

Die Schufa verwies zu rechtlichen Fragen auf eine Pressemitteilung, wonach die Einwilligung für „Schufa Check Now" ebenso wie die weitere Verarbeitung von Daten freiwillig sei. Eine Datenverarbeitung der Kontoauszüge finde zudem nur statt, „wenn der Verbraucher – und zwar ausdrücklich und unabhängig von der eigentlichen Dienstleistung – eine gesonderte Einwilligung" erteile. Welchen Vorteil Kunden von einer solchen Datenspende haben, die nichts mit der Dienstleistung zu tun hat, erklärte die Schufa nicht.

• Rückzug

Nachdem Medien über den Test kritisch berichtet hatten, ruderten alle Testbeteiligten zurück: „Dabei fließen aktuell noch keine Daten", sagte Schufa-Vorstandsmitglied Ole Schröder. Schröder war, bevor er zur Schufa gegangen war, Staatssekretär im Bundesinnenministerium. Und Telefónica/O2 erklärte am Tag nach der Medienberichterstattung: „Die Ergebnisse dieses Tests haben unsere Erwartungen leider nicht erfüllt. Daher hat Telefónica/O2

heute beschlossen, den Test zu beenden und das ´CheckNow´-Verfahren der Schufa nicht mehr länger zu nutzen."

An dem Pilotprojekt hatten demnach etwa 100 Menschen freiwillig teilgenommen. Dazu mussten sie der Schufa ausdrücklich einen Auftrag erteilen. Der Konzern betonte: „Das Verfahren bietet die Schufa den Verbrauchern in komplett eigener datenschutzrechtlicher Verantwortung an." Die genutzten Kontoinformationen seien nicht gespeichert worden.

Schufa-Vorstand Schröder betonte: „Sensible Daten wie beispielsweise die Bezahlung einer Arztrechnung werden automatisch herausgefiltert und dürfen nicht verarbeitet werden." Die gespeicherten Kontodaten beschränken sich nach Auskunft des Unternehmens ausschließlich auf relevante Daten zur Bonitätsbewertung und Betrugsbekämpfung. Mit der freiwilligen Daten-Speicherung könne der Verbraucher weitere zukünftige Kontozugriffe durch Dritte vermeiden und seine Daten dennoch für ihn vorteilhaft in eine Schufa-Bonitätsbewertung einfließen lassen. Die Kontoanalyse finde nur einmal bei der Schufa statt: „Ziel ist es, dass Verbraucher von aktuellen positiven Kontoinformationen auch für zukünftige Transaktionen und Bonitätsabfragen profitieren können. Die Daten sind dadurch aktueller, und wir erfüllen so auch Forderungen von Verbraucherschützern." Für Verbraucher, die keinen Auftrag zum Einblick ins Konto erteilten, bleibe es bei der klassischen Bonitätsprüfung. „Fällt die Bewertung nach den Kontodaten negativ aus, kann der Verbraucher seine Einwilligung widerrufen." Es bleibe dann bei der klassischen Bonitätsprüfung. „Aus unserer Sicht ist es für Verbraucher besser, die Schufa sammelt als neutrale Instanz die Daten treuhänderisch, als Unternehmen, die damit unmittelbar Geschäfte machen."

• Zahlungsdiensterichtlinie PSD 2

Seit Einführung der Zweiten EU-Zahlungsdiensterichtlinie (PSD2) und deren nationaler Umsetzung im Zahlungsdiensteaufsichtsgesetz (ZAG) ist es möglich, dass Drittanbieter wie Finanz-Start-ups Einblick auf Konten bekommen können. Voraussetzung ist, dass der Kunde dem zustimmt. Die Schufa hatte für derartige Aktivitäten den Münchner Kontoinformationsdienst FinAPI GmbH gekauft. Schröder zufolge handelt es sich bei dem Vorhaben um ein in Europa inzwischen gängiges Verfahren, „das auch andere Auskunfteien seit geraumer Zeit einsetzen". Die Schufa sei ständig in enger Abstimmung mit den Datenschutzbehörden. „Sie wurden vor dem Test informiert, zustimmen müssen die Datenschützer nicht."

Ein Sprecher des Bundesjustizministeriums sagte, dieses neue Geschäftsmodell werfe rechtliche Fragen auf. Daher werde sich das Ministerium, das davon erst jetzt erfahren habe, dies „genau anschauen". Schließlich gehe es hier um „besonders sensible Daten", und die Verbraucher müssten stets in der Lage sein zu verstehen, wofür sie jeweils ihre Einwilligung erteilen.

Die Grünen-Politiker Tabea Rößner und Konstantin von Notz kritisierten, die Schufa habe bereits heute Zugriff auf weitreichende Informationen über die Verbraucher, „die selbst nach wie vor nicht nachvollziehen können, wie und auf welche Weise diese Daten für den persönlichen Score gewichtet werden". Der stellvertretende FDP-Fraktionsvorsitzende Stephan Thomae sagte, es sei alarmierend, dass die Schufa Kontoauszüge der Verbraucher durchleuchten wolle: „Für niedrigere Preise und mehr Möglichkeiten im Rechtsverkehr sollen die Bürger mit ihren Daten bezahlen." Wenn Bürger am Ende nur durch die Einwilligung in diese Datenverarbeitung durch die Schufa einen Handy- oder Mietvertrag abschließen könnten, hätten sie faktisch keine freie Wahl mehr (Wischmeyer, Zeigt her eure Konten, SZ 27.11.2020, 17; CheckNow: Kritik an Schufa-Angebot zur Datennutzung – Telefónica beendet Test, www.heise.de 28.11.2020, Kurzlink: https://heise.de/-4973668).

Bundesweit

Generali bietet Gesundheitsanalyse per Gesichtsscan

Der private Krankenversicherer Generali will im Jahr 2021 mit einer App auf den Markt kommen, die in zwei Minuten durch die Analyse der Blutgefäße im Gesicht die Sauerstoffsättigung des Blutes, Atem- und Herzfrequenz sowie die Herzfrequenz-Variabilität misst. Mit Hilfe eines Programms, das Verfahren der künstlichen Intelligenz nutzt, sollen die Daten analysiert und die Ergebnisse auf dem Smartphone ablesbar gemacht werden.

Für das Angebot hat sich die Generali Deutschland mit dem israelischen Start-up Binah.ai und der Beratungsfirma SDG Group zusammengetan. Die Technik hinter der Untersuchung heißt „Remote Photoplethysmographie". Plethys heißt auf Altgriechisch „Fülle", „Graphie" heißt schreiben. Das Verfahren zeichnet kontaktlos mit der Kamera die Füllung der Blutgefäße auf. Eine ähnliche Technik verwendet bereits eine Reihe von Versicherern weltweit, zum Beispiel der chinesische Anbieter Ping An. Auf dem deutschen Markt wird die Generali mit der App, die vier wichtige Parameter misst, voraussichtlich der erste Anbieter sein. Die App soll mit einem Angebot gebündelt werden, das „VitalSigns & Care" genannt wird. Kunden kaufen mit der App bei Generali Assistance-Dienstleistungen in der Gesundheitsfürsorge, Hilfe im Haushalt, bei Pflege und bei Reisen. Wie teuer das wird, steht noch nicht fest. Die App ist kein Medizinprodukt, sondern wird als „Selbstüberwachungsinstrument" angeboten. Deshalb benötigt die Generali dafür keine Zulassung durch das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM).

Mit dem System versucht die Generali, sich als Partner im Alltag der Kunden zu etablieren. Versicherer haben das Problem, dass außer beim Abschluss einer Police, der Prämienzahlung und einem möglichen Schaden sie kaum Kontakt zu ihren Kunden haben. Bei privaten Krankenversicherern beschränkt sich die Kommunikation auf die Einreichung von Rechnungen oder Rezepten und die Erstattung. Weil Online-Portale wie Check24 und Verivox auf dem Vormarsch sind und auch die Internet-Giganten Amazon und Apple sich mit Finanzdienstleistungen und Versicherungen befassen, befürchten die Versicherungsgesellschaften den Kontakt

zu ihren Kunden ganz zu verlieren und zu reinen Zulieferern zu werden.

Die Antwort der Versicherer heißt im Branchenjargon „Ökosystem". Die Kunden sollen durch umfassende Dienstleistungen an die Gesellschaften gebunden werden. Generali-Deutschlandchef Giovanni Liverani hat die Devise ausgegeben, dass seine Gesellschaft „Lifetime Partner" der Kunden, deren lebenslanger Partner werden möchte. Dass dies kein einfaches Unterfangen ist, hat die Generali schon erfahren, als sie 2016 das in Südafrika entwickelte Versicherungsprogramm Vitality auf den Markt gebracht hat: Eine App überwacht Fitnessaktivitäten und Einkaufsverhalten, als Belohnung gibt es Gutscheine von Adidas oder Amazon und Nachlässe auf die Versicherungsprämie. Bislang scheint Vitality kein großer Erfolg zu sein; das Unternehmen weigert sich hartnäckig Nutzerzahlen zu nennen.

Der Trend zu mehr gesundheitlicher Vorsorge verstärkt sich; dafür sorgt auch die Covid-19-Pandemie. Dabei spielen digitale Hilfsmittel eine immer größere Rolle. Uhren messen die Herzfrequenz und den Herzrhythmus, zahlreiche Apps auf Smartphones helfen bei der Überwachung des eigenen Körpers. Eine repräsentative Umfrage der Berliner Marktforschungsfirma EPatient Analytics hat ergeben, dass 26% der Bevölkerung, die das Internet nutzen, über eine App zu den Themen Ernährung, Sport und Entspannung verfügen oder an einem Online-Kurs teilgenommen haben. Immerhin 14% - das sind 9,8 Millionen Menschen - verfügen über eine App, mit der über das Mobiltelefon Puls, Blutdruck oder Hautveränderungen erfasst werden können.

Die Generali rechnet sich Chancen wegen ihrer besonderen Technik aus. Allerdings ist der Markt stark in Bewegung. Private und gesetzliche Krankenversicherer arbeiten an Lösungen, um die Kunden digital zu unterstützen. Im Dezember 2019 ist das „Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation" in Kraft getreten, nach dem Ärzte Gesundheits-Apps verschreiben dürfen. Die fünf ersten Apps hat das BfArM inzwischen zugelassen. Die Generali wird keine Zulassung suchen (Fromme, Ein Blick in die Augen, SZ 24.11.2020, 18).

Hessen

Alexander Roßnagel zum Datenschutzbeauftragten gewählt

Der hessische Landtag hat am 10.12.2020 den Juristen Professor Alexander Roßnagel mit großer Mehrheit zum Datenschutzbeauftragten gewählt. Roßnagel soll von März 2021 an als ein ausgewiesener Datenschutzfachmann der „Hüter des Grundrechtes auf informationelle Selbstbestimmung" in dem Bundesland werden. Neben den Regierungsfraktionen von CDU und Grünen stimmten auch die FDP, die Linke und die AfD für ihn. Die SPD-Fraktion enthielt sich. Sie hatte im Vorfeld moniert, dass Schwarz-Grün den Nachfolger für den Amtsinhaber Michael Ronellenfitsch im Alleingang bestimmt und nur einen Kandidaten vorgeschlagen habe. Ronellenfitsch hatte seit 17 Jahren die Position inne und hält damit bundesweit einen Rekord.

Roßnagel lehrt aktuell als emeritierter Professor für öffentliches Recht, Recht der Technik und des Umweltschutzes an der Universität Kassel. Er leitet dort schon seit Jahren die Projektgruppe verfassungsverträgliche Technikgestaltung (Provet) und ist Direktor des Wissenschaftlichen Zentrums für Informationstechnikgestaltung. Der 70-Jährige ist zudem Sprecher des Forschungsverbunds Forum Privatheit, den das Bundesforschungsministerium fördert. Roßnagel erklärte nach seiner Wahl: „Die zunehmende Digitalisierung aller Lebensbereiche führt zu immer intensiveren Verarbeitungen personenbezogener Daten und damit zu Eingriffen in die informationelle Selbstbestimmung." Zugleich werde es so schwerer, Risiken für Grundrechte zu erkennen und sich gegen Eingriffe in Grundrechte zu wehren. Während die Daten verarbeitenden Stellen in Wirtschaft und beim Staat immer mehr über die Bürger wüssten, werde die Datenverarbeitung für diese immer intransparenter.

In seiner neuen Rolle will Roßnagel mit seiner unabhängigen Behörde soweit wie möglich für Schutz und Machtausgleich sorgen. In einer technikgeprägten Welt gelinge dies am effektivsten, wenn der Datenschutz bereits in den informationstechnischen Systemen eingebaut sei; er plädiert für Privacy by Design. Was an Grundrechtseingriffen technisch gar nicht erst möglich sei brauche nicht mehr verboten, verfolgt und sanktioniert zu werden. Es sei wichtig Transparenz über die Verarbeitung personenbezogener Daten herzustellen sowie Datenverarbeiter, Betroffene und die Öffentlichkeit über Risiken, Vorgaben, Garantien und Rechte aufzuklären und zu sensibilisieren. Mit seinen bisherigen Tätigkeiten will er eng verbunden und beim „Forum Privatheit" an Bord bleiben, eine enge Kooperation zwischen Forschung und Aufsichtsbehörden sei „wichtig und notwendig".

Roßnagel prägt seit Jahrzehnten die hiesige Debatte über die Privatsphäre. 2001 legte er zusammen mit dem 2010 verstorbenen Dresdner Informatikprofessor Andreas Pfitzmann sowie dem früheren Berliner Beauftragten für Datenschutz und Akteneinsicht, Hansjürgen Garstka, ein in Fachkreisen vielbeachtetes Gutachten im Auftrag des Bundesinnenministeriums zur Reform des Bundesdatenschutzgesetzes vor. Datenschutz durch Technik und ein Recht auf anonymen Internetzugang waren schon damals Stichworte. Der damalige Innenminister Otto Schily (SPD) ließ das Werk aber rasch in der Schublade verschwinden.

Roßnagel wirbt für einen besseren Schutz vor Profiling und für einen einheitlichen Beschäftigtendatenschutz. Bei der Datenschutz-Grundverordnung (DSGVO) machte er sich wiederholt für Korrekturen stark. Jüngst bezeichnete er die Corona-Warn-App als gute Möglichkeit, um die Gesundheit zu schützen und Freiheitsbeschränkungen zu lockern. Zugleich mahnte er auch im Kampf gegen die Pandemie das Sammeln und Analysieren von Massendaten auf ein Minimum zu beschränken.

Der Grünen-Fraktionschef Mathias Wagner freute sich über die Wahl. Bei seiner Vorstellung sei erkennbar gewesen, dass Roßnagel „die vielschichtigen Aspekte des Themas nicht nur bearbeiten, sondern auch weiterentwickeln will". Er knüpfe „damit an die große Tradition an, die Hessen beim Thema Datenschutz hat". In dem Bundesland wurde vor 50 Jahren in einer weltweiten Premiere ein Datenschutzgesetz beschlossen. Auch

der Datenschutzexperte der FDP-Fraktion, Jörg-Uwe Hahn, freute sich: „Wir wollen die Digitalisierung zum Nutzen der Menschen gestalten, nicht um sie zu überfordern, zu kontrollieren oder gar zu manipulieren. Hier ist ein scharfes juristisches Auge sehr wichtig" (Krempl, Hessen: Privacy-Experte Roßnagel wird Landesdatenschutzbeauftragter, www.heise.de 12.12.2020, Kurzlink: https://heise.de/-4987739).

Hessen

Tegut etabliert kassiererlose Kleinstshops

Die Handelskette Tegut mit Sitz in Fulda hat am 05.11.2020 testweise einen Supermarkt eröffnet, der ohne Personal auskommt und rund um die Uhr geöffnet ist. In der osthessischen Stadt ist der kleine Laden mit 50 Quadratmeter Verkaufsfläche aufgebaut worden, in dem es 950 Produkte für den täglichen Bedarf gibt. Den Zugang verschaffen sich die Kunden, indem sie eine App des Unternehmens herunterladen; mit einem QR-Code verschafft man sich dann Eintritt. Mit der App lässt sich auch zahlen, außerdem ist es mit Kreditkarten und der Girocard möglich. In jedem Fall müssen die gekauften Produkte gescannt werden. Der kleine Laden wird mit mehreren Kameras und 3D-Sensoren überwacht.

Die Handelskette Tegut, die zum schweizerischen Migros-Konzern gehört, unterhält vorwiegend in Hessen und Thüringen 270 konventionelle Supermärkte, die stärker als die anderer Ketten auf Bioprodukte und regionale Waren ausgerichtet sind. Mit den automatisierten Läden, die als „tegut… teo" firmieren, will man neue Kundenkreise erschließen, die auf dem Weg zur Arbeit oder nach Hause ohne viel Aufwand einkaufen wollen, wonach ihnen gerade ist. Das Konzept sei „die stationäre Antwort auf Onlineshopping".

Von „Einkaufen ohne Planung, Anfahrtswege, Zeitverlust" ist in einer Pressemitteilung des Unternehmens die Rede. Tegut möchte eine Reihe solcher Geschäfte etablieren, die unter anderem in „städtischen Zwischenräumen" aufgestellt werden sollen, etwa an Verkehrsknotenpunkten, vor öffentlichen Einrichtungen oder auch auf dem Gelände größerer Unternehmen, in Neubaugebieten, vor Kliniken und Universitäten, auf Firmengeländen – überall dort, wo der klassische Supermarkt zu groß ist. Bis Ende 2021 sind bis zu zehn „tegut… teo"-Geschäfte geplant (Köhler, Ein Supermarkt ohne Kassierer, www.faz.net 05.11.2020; Tegut testet Laden ohne Kassierer, SZ 06.11.2020, 24).

Niedersachsen

LfD untersagt Amazon automatisierte Leistungskontrolle

Niedersachsens Chef-Datenschützerin Barbara Thiel untersagte Amazon teilweise die Nutzung einer zentralen Software, mit der die Mitarbeiter minutengenau überwacht werden können. Amazon will dagegen klagen.

Im dritten Quartal des Jahres 2020 hat Amazon fast 100 Milliarden Dollar Umsatz gemacht – eine Steigerung im Vergleich zum Vorjahresquartal um 37%. Amazon zählt damit nicht nur zu den großen Gewinnern der Corona-Pandemie, sondern auch zu den wertvollsten Unternehmen der Welt. Doch der Online-Gigant steht seit Jahren für den Umgang mit seinen Angestellten in der Kritik, insbesondere hinsichtlich ihrer Überwachung.

Die niedersächsische Landesbeauftragte für den Datenschutz (LfD) Barbara Thiel beanstandete einige Funktionen der von Amazon eingesetzten Software, mit der die Leistung der Mitarbeiter offenbar permanent kontrolliert werden kann. Der Amazon-Arbeiter scannt jedes Teil, das er einlagert, heraussucht oder in ein Paket packt. Dieser Scan-Vorgang wird sekundengenau aufgezeichnet und einem Vorarbeiter angezeigt. So kann dieser jeden Arbeitsschritt der Beschäftigten überwachen und sehen, ob ein bestimmter Arbeiter auch genügend Pakete packt. Ein Vorarbeiter schilderte, wie er auf seinem Display sieht, wenn ein Mitarbeiter mal für wenige Minuten nicht arbeitet.

Die LfD bestätigte, dass sie dem Amazon-Standort im niedersächsischen Winsen untersagt hat „ununterbrochen jeweils aktuelle und minutengenaue Quantitäts- und Qualitätsleistungsdaten ihrer Beschäftigten zu erheben und diese zu nutzen". In Winsen steht eines der modernsten Amazon-Zentren in Europa. Amazon nutzt die Software bundesweit. Ein Amazon-Sprecher teilte mit, dass man den Bescheid nicht akzeptiere: „Anders als die Behörde sind wir der Meinung, dass auch die Art und Weise der Datenerhebung rechtmäßig ist. Deshalb werden wir die Entscheidung der Behörde gerichtlich überprüfen lassen."

Der Kommentar von André Scheer von der Gewerkschaft ver.di: „Die Totalüberwachung durch Amazon ist das genaue Gegenteil von guter und sicherer Arbeit." Für Scheer steht die permanente Kontrolle der Mitarbeiter im Zusammenhang mit dem Beschäftigungsmodell bei Amazon. Gerade im Weihnachtsgeschäft stelle Amazon Tausende Arbeiter befristet ein: „Da wird dann ausgesiebt." Nur die Schnellsten dürften bleiben oder wiederkommen. Die Folge: Der Druck auf alle Beschäftigten steige und damit auch die Angst unter den Beschäftigten negativ aufzufallen.

Ein Vorarbeiter bestätigte diese Praxis. Sieht er, dass die Rate eines Mitarbeiters fällt, soll er eingreifen: „Dann gehe ich dahin, gucke, ist der Mitarbeiter da, und schaue: Was ist das Problem? Unterhält er sich vielleicht zu lange, ist er nicht am Platz, zu oft auf der Toilette?" Der Vorarbeiter berichtete auch, dass durch die Software detaillierte Profile jedes einzelnen Beschäftigten erstellt werden. Fällt die Rate eines Beschäftigten dauerhaft, werde dieser zum Gespräch gebeten. Ob ein befristet Beschäftigter eine Vertragsverlängerung bekommt, hängt dem Vorarbeiter zufolge auch davon ab, ob er die Rate erfülle. Der Umweltorganisation Greenpeace liegen Dokumente vor, die diese Darstellung untermauern.

Amazon teilte dazu mit: „Wir bieten gute Bezahlung und eine Arbeitsumgebung, in der Menschen erfolgreich sind, ihren Karriereweg finden und Kunden zufrieden stellen." Ob Amazon für den Einsatz der Software zusätzlich auch ein Bußgeld zahlen muss, ist noch nicht entschieden. Die Behörde in Niedersachsen geht allerdings davon aus, dass

auch in diesem Sinn ein Verfahren eingeleitet werde (Friedrich/Jolmes, Verfahren gegen Amazon, www.tagesschau.de 01.12.2020).

Niedersachsen

10,4 Mio. Geldbuße gegen notebooksbilliger.de wegen Videoüberwachung

Die Landesbeauftragte für den Datenschutz (LfD) Niedersachsen hat Anfang Januar 2021 eine Geldbuße in Höhe von 10,4 Mio € gegenüber der notebooksbilliger.de AG ausgesprochen, weil das Unternehmen über mindestens zwei Jahre seine Beschäftigten illegal per Video überwachte. Die unzulässigen Kameras erfassten unter anderem Arbeitsplätze, Verkaufsräume, Lager und Aufenthaltsbereiche. Das Unternehmen rechtfertigte die Überwachung mit der Verhinderung und Aufklärung von Straftaten sowie der Kontrolle des Warenflusses in den Lagern. Bei notebooksbilliger.de war keine Beschränkung der Videokontrolle auf einen bestimmten Zeitraum oder konkrete Beschäftigte erfolgt, wie es gesetzlich bei der Straftatbekämpfung gefordert wird. Die Aufzeichnungen wurden in vielen Fällen 60 Tage und damit deutlich länger als erforderlich gespeichert.

Gemäß der LfD Barbara Thiel genügt ein Generalverdacht nicht: „Wir haben es hier mit einem schwerwiegenden Fall der Videoüberwachung im Betrieb zu tun. Sie kann nach der Rechtsprechung des Bundesarbeitsgerichts dazu führen, dass die Betroffenen den Druck empfinden sich möglichst unauffällig zu benehmen, um nicht wegen abweichender Verhaltensweisen kritisiert oder sanktioniert zu werden." Auch Kundinnen und Kunden von notebooksbilliger.de waren von der unzulässigen Videoüberwachung betroffen; einige Kameras waren auf Sitzgelegenheiten im Verkaufsraum gerichtet. Dort halten sich Menschen oft länger auf, zum Beispiel um die angebotenen Geräte zu testen (Presseerklärung der LfD Nds. V. 08.01.2021, LfD Niedersachsen verhängt Bußgeld über 10,4 Millionen Euro gegen notebooksbilliger.de).

Datenschutznachrichten aus dem Ausland

Weltweit

Amazon schnüffelt gegen Kritiker von innen und außen

Amazon treibt hohen Aufwand, um eigene Mitarbeiter, Gewerkschafter und soziale Bewegungen zu überwachen. Auch Vertragspartner, Diebe, Drogendealer und Umweltschützer sind im Visier, selbst wenn sie gar nichts mit Amazon zu tun haben. Laut einer Konzernsprecherin geschieht das alles legal und mit Wissen der örtlichen Behörden: „Jeder Versuch diese Aktivitäten aufzubauschen oder zu unterstellen, dass wir etwas Ungewöhnliches oder Falsches tun, ist unverantwortlich und falsch."

Die US-Webseite „Motherboard" hatte mehr als zwei Dutzende interne Berichte Amazons zugespielt bekommen, deren Echtheit Amazon nicht bestreitet. Demnach verzeichnet Amazon nicht nur öffentliche Aktionen, vom Verteilen von Flugblättern bis zum Streik, genau mit Zeitpunkt, Ort und Zahl der Teilnehmer, sondern auch nicht-öffentliche Treffen von Arbeitnehmern mit Gewerkschaftern. Wichtige Informationsquellen sind Äußerungen in sog. Sozialen Netzwerken, sei es von Mitarbeitern oder Außenstehenden. Dabei bedient sich Amazon der Dienstleistungen Dritter, die sich Zutritt zu geschlossenen Foren verschaffen. Die Betroffenen werden darüber freilich nicht informiert; Amazon ist daran gelegen diese Schnüffelei geheim zu halten.

Beschwerden von Mitarbeitern werden ebenso erfasst wie Diebstähle. Zusätzlich wird die Kriminalität in der Region untersucht. Motherboard nennt als Beispiel den Drogenhandel. Amazon möchte wissen, ob der den eigenen Betrieb stören könnte und ob Amazon-Mitarbeiter selbst Drogen nehmen könnten. Unter dem Punkt „Betriebsumgebung" werden unter anderem politische Ereignisse analysiert, wie zum Beispiel die Gelbwesten-Bewegung in Frankreich oder eine Demonstration in Wien, die gegen die Politik der Regierung des Iran gerichtet war. Gleichzeitig hat Amazon besonderes Interesse an Umweltschützern. So wird der Erfolg Amazon-kritischer Greenpeace-Videos an Likes und Weiterverbreitungsstatistiken gemessen. Amazon nimmt auch die von Greta Thunberg inspirierte Bewegung Fridays For Future als Bedrohung wahr. Sie gewinnt „an Einfluss insbesondere auf junge Menschen und Studenten" und „zieht immer mehr Menschen schnell an", wie es in einem der Dokumente heißt.

Detektive werden ebenfalls eingesetzt, nach Angaben Amazons zum Schutz von Werttransporten. Aus den Dokumenten geht hervor, dass Detektive in ein polnisches Lager eines Amazon-Dienstleisters eingeschleust wurden. Sie sollten Vorwürfen unpassender Einstellungsverfahren nachgehen, konnten diese aber nicht erhärten (Sokolov, Amazon überwacht Gewerkschaftler, Greenpeace und Greta-Fans, www.heise.de 25.11.2020, Kurzlink: https://heise.de/-4970229).

Weltweit

Clubhouse und der Datenschutz

Die Social-Audio-App Clubhouse – die zunächst nur als sogenannte Beta-Version ausgeliefert wurde – erfreut sich von Anbeginn großen Zuspruchs. Die App versucht die Intimität von Clubabenden zu suggerieren. Dabei ist sie unkontrollierbar öffentlich.

Das musste etwa Thüringens Ministerpräsident Bodo Ramelow (Die Linke) erfahren, der sich am 22.01.2021

in einem Clubhouse-Talk wohl wie an einer Hotelbar fühlte und angeregt plauderte, wobei ihm gleich mehrere Fauxpas unterliefen: Er nannte die Bundeskanzlerin „Merkelchen" und war veranlasst sich dafür später zu entschuldigen. Zum anderen offenbarte er, dass er während der langen Bund-Länder-Beratungen zur Coronakrisenbekämpfung gelegentlich das Handy-Spiel Candy Crush zockt. Für ihn war es ein Kommunikationsdesaster.

Die Beliebtheit der App führte dazu, dass sie Anfang 2021 eine Woche lang auf Platz eins in Apples App-Store stand. Nur iPhone-Besitzer konnten sie zunächst nutzen. Besitzer von Android-Smartphones bleiben vorerst außen vor. Die beiden Firmengründer Paul Davison und Rohan Seth kündigten aber an, dass die App künftig auch auf Smartphones mit dem Google-Betriebssystem zu finden sein wird. Dann können auch die nach Milliarden zählenden Android-Nutzer drauflos erzählen.

Zutritt zum Clubhouse bekommt man nur, wenn man von einem Teilnehmer eingeladen wird. Jeder neue Nutzer darf zwei Einladungen an seine Freunde verschicken. Wer zu diesem exklusiven Kreis gehört, kann dann unter hunderten Konferenzen aussuchen, die parallel stattfinden und auch zwischen den Talks wechseln. Annabel Oelmann, Vorständin der Verbraucherzentrale Bremen, erklärte, man müsse sich Clubhouse vorstellen wie eine kleine Talkshow – nur ohne Bilder. Die App ist eine reine Audioplattform, in der die Nutzer und Nutzerinnen „Rooms" oder „Räume" erstellen, innerhalb dieser man mit allen reden und diskutieren kann.

Unter ihnen sind Promis, Politiker und Journalisten. Oelmann empfiehlt, bei all dem Hype eine grundsätzliche Vorsicht in puncto Datenschutz nicht abzulegen: Bei der Registrierung müssen die Nutzer den Zugriff auf alle gespeicherten Kontakte erlauben. Nur dann darf man Einladungen an seine Freunde verschicken: „So besteht die Gefahr, dass Schattenprofile erstellt und zu Werbezwecken genutzt werden." Dies sei aber nach Artikel 14 der Datenschutz-Grundverordnung (DSGVO) nicht zulässig, da die betroffenen Kontakte nicht vorab über die Nutzung ihrer persönlichen Daten informiert werden.

Ein weiterer Kritikpunkt der Verbraucherschützerin ist, dass alle Gespräche temporär aufgezeichnet werden können, wenn etwa während des Live-Gesprächs ein Regelverstoß gemeldet wird: „Wer dann aber Zugriff auf die Gesprächsinhalte bekommt und wer und wann über die Löschung der Gespräche entscheiden wird, bleibt im Dunkeln." Zudem sammelt Clubhouse Daten, um Kommunikationsprofile zu erstellen, also etwa Informationen darüber, mit welchen Accounts und Gruppen man sich austauscht, wie oft und wie lange man aktiv ist und zu welchen Tageszeiten.

Die Datenschutzbestimmungen von Clubhouse sind, so Oelmann, nicht klar formuliert: „Es bleiben viele Fragen offen, welche Daten für welche konkreten Zwecke erhoben und verarbeitet werden." Das aber sollte nach dem datenschutzrechtlichen Transparenzgebot selbstverständlich sein. Ihre Schlussfolgerung: Clubhouse sei eine Datenkrake. Wer die App nutze, zahle dafür nicht nur mit den eigenen persönlichen Daten, sondern gebe auch die persönlichen Daten von Familie, Freunden und Bekannten preis. Oder eben, was man so treibt in der Ministerpräsidentenrunde bei der Kanzlerin (Scholtes, Clubhouse und die Sache mit dem Datenschutz, www.dw.com/de/ 26.01.2021).

USA – Weltweit

Facebook agitiert gegen Apples Tracking-Opt-in

Hunderte Millionen iPhone-Besitzer werden bald nach ihrer Einwilligung gefragt, bevor Apps bestimmte Daten sammeln dürfen. Das versetzt Facebook in Panik. Glaubt man Facebook, geht es um das Schicksal von Millionen kleinen Unternehmen, ja mehr als das: die Zukunft des Netzes stehe auf dem Spiel. Nutzerinnen und Nutzern von Apple-Anwendungen wird bald ein unscheinbarer Dialog präsentiert werden, in dem bei ihnen nachfragt wird, ob Apps ihre Daten sammeln dürfen.

In mehreren Blogeinträgen und ganzseitigen Anzeigen in großen US-Medien inszenierte sich Facebook als Retter des „freien Internets" und Fürsprecher kleiner und mittelständischer Unternehmen (KMUs). Auf einer eigens eingerichteten Kampagnenseite sollen Hoteliers, Friseure, Restaurantbesitzerinnen und andere angeblich Betroffene ihre Stimme gegen Apple erheben und auf die dramatischen Folgen aufmerksam machen. Juni 2020 hatte das „App Tracking Transparency"-Framework (ATT) angekündigt, dass Entwicklerinnen und Entwickler um Erlaubnis fragen müssen, bevor sie User quer über andere Apps und Webseiten hinweg verfolgen. Wer das nicht will, muss bislang aktiv widersprechen.

Apple verhindert also standardmäßiges Tracking und macht daraus eine Opt-in-Option, so wie dies die europäische Datenschutz-Grundverordnung auch gesetzlich verlangt. Es braucht die ausdrückliche Zustimmung der Nutzenden, bevor ihnen eine individuelle Werbe-Identifikationsnummer zugewiesen werden darf. Das hat erhebliche Auswirkungen. Der Mensch ist ein Gewohnheitstier, was Unternehmen bisher im Netz gnadenlos ausnutzen: Nur ein Bruchteil der Nutzerinnen und Nutzer beschäftigt sich mit den Voreinstellungen der Dienste und Apps, die sie installieren. Die Standardkonfiguration bleibt unangetastet, und die lautet meist, dass alle Datenschleusen geöffnet sind.

Wenn Webseiten Bestätigungsdialoge einblenden, sind die meist schwer verständlich bis manipulativ: Wollen Sie alle Cookies akzeptieren? Dann klicken Sie bitte auf diesen riesigen blauen Knopf. Sie haben etwas dagegen? Na gut, hier sind 27 Haken, die Sie einzeln abwählen können.

Derartige sog. Dark Patterns sollen Menschen dazu bringen, Dingen zuzustimmen, die sie gar nicht wollen. Der Dialog, den bald Hunderte Millionen iPhone-Besitzer sehen werden, soll nicht irreführend, sondern eindeutig sein. Darunter gibt es nur zwei gleich große Optionen: „Ask App not to Track" oder „Allow". Die genauen deutschen Übersetzungen sind noch nicht bekannt, sie dürften aber ähnlich unmissverständlich ausfallen.

Die geplanten Änderungen versetzen nicht nur Facebook in Aufregung, sie bedrohen eine ganze Branche, die jedes Jahr Milliarden Dollar umsetzt. Werbenetzwerke, Targeting-Firmen und Anbieter von Tracking-Technologie sehen

ihr Geschäftsmodell in Gefahr. Auch viele Entwicklerinnen und Entwickler integrieren Facebooks Software-Bausteine in ihre Apps, sammeln darüber wertvolle Nutzungsdaten und blenden personalisierte Anzeigen ein. Gemeinsam mit Facebook, großen Verlagen und der Werbebranche protestierten sie gegen Apples Pläne.

Der Widerstand zeigte Wirkung: Apple verschob den Start, woraufhin acht Organisationen wie Amnesty International und die Electronic Frontier Foundation (EFF) einen offenen Brief schrieben, um ihrer Enttäuschung Ausdruck zu verleihen. Jane Horvath, die bei Apple für alle Entscheidungen zuständig ist, die Datenschutz betreffen, antwortete umgehend: „Wir stehen weiter voll und ganz hinter ATT und unserem umfassenden Ansatz Privatsphäre zu schützen." Apple habe den Entwicklern nur mehr Zeit geben wollen, um ihre Apps anzupassen.

Diese Schonfrist geht bald zu Ende. In Foren tauchen erste Screenshots auf, die den Bestätigungsdialog zeigen. Offenbar wird es Apple Entwicklern Anfang 2021 verbieten, ohne Einwilligung mithilfe einer Werbe-ID zu tracken. Für Apple-Chef Tim Cook ist die Sache gemäß einer Twitternachricht eindeutig: „Wir glauben, dass User selbst entscheiden sollten, welche Daten über sie gesammelt werden." Facebook könne Nutzerinnen und Nutzer nach wie vor quer über Apps und Webseiten hinweg verfolgen. „ATT in iOS 14 verlangt bloß, dass sie davor um Erlaubnis fragen."

Wie glaubwürdig Cooks Bekenntnis für den Datenschutz ist, bleibt unklar: Zwar werden bei Apples Messenger-Dienst die Daten verschlüsselt übertragen. Doch wer eine Sicherheitskopie auf Apples iCloud anlegt, muss auf den Konzern vertrauen, denn auch der hat dann einen Schlüssel. Die Entscheidung soll Gerüchten zufolge auf Betreiben des FBI zustande gekommen sein.

Cook und Facebook-Chef Mark Zuckerberg verbindet eine innige Abneigung. Cook reibt Zuckerberg bei jeder Gelegenheit unter die Nase, wie wenig er von Facebooks Geschäftsmodell hält: Daten sammeln, Nutzerprofile bilden und deren Aufmerksamkeit an Werbetreibende verkaufen, die personalisierte Anzeigen schalten können. Zuckerberg betont seinerseits, dass Facebook Milliarden Menschen auf der ganzen Welt vernetze, die keinen Cent dafür zahlen müssten. Apple verkaufe hochpreisige Geräte an eine wohlhabende Elite. Cook solle sich nicht als Held aufspielen, der Menschen ihre Privatsphäre zurückgebe.

Tatsächlich verdient Apple den Großteil seines Geldes mit Hardware. Das letzte Quartal 2020 war für Apple äußerst erfolgreich: Apple verkaufte weltweit mit 90,1 Mio. Stück am meisten Smartphones. Dagegen macht das Anzeigengeschäft fast 99% von Facebooks Umsatz aus. Der aktuelle Konflikt ist für Zuckerberg doppelt unangenehm: Zum einen trifft Apple Facebook an seiner wundesten Stelle. Zum anderen nutzt Cook genau die gleichen Wörter, mit denen Facebook sonst oft argumentiert: Kontrolle und Wahlfreiheit. Wir geben Nutzerinnen und Nutzern doch nur eine Wahl. Wer will, kann sich gern überwachen lassen. Wir geben Nutzerinnen und Nutzern doch nur eine Wahl, sagt Zuckerberg. Wer will, kann gern widersprechen.

Deshalb versucht Facebook, das „freie Internet" und KMUs für seine Interessen zu instrumentalisieren. Viele Webseiten und Dienste sind nur deshalb gratis, weil sie sich durch Werbung finanzieren. Doch Apple will nicht Anzeigen per se verbieten, sondern nur das personalisierte Tracking. Werbung, die KMUs auf Facebook schalten, wäre wohl weniger zielgerichtet und effektiv, wenn viele Menschen dem Tracking widersprechen. Doch dass ausgerechnet Facebook, das jahrelang mit Programmen wie Free Basics aktiv daran gearbeitet hat, das freie Netz durch ein Facebook-Internet zu setzen, sich nun als Bastion des freien Netzes aufspielt, ist zumindest verwunderlich.

Das sehen nicht nur die Bürgerrechtler der EFF kritisch, sondern auch Facebooks eigene Angestellte, die sich in internen Chats skeptisch äußern, so z.B. ein Entwickler: „Es fühlt sich an, als rechtfertigten wir es, dass wir schlechte Dinge tun, indem wir uns hinter Leuten verstecken, die mehr Mitgefühl auslösen." Oder ein anderer Mitarbeiter: „Machen wir uns keine Sorgen, dass uns das auf die Füße fällt, weil es so aussieht, als wolle Facebook nur sein eigenes Geschäft verteidigen?"

Für Facebook steht viel auf dem Spiel. In den USA und Europa drohen Kartellklagen und scharfe Regulierung, die den Umsatz empfindlich schmälern könnten. Der neue US-Präsident Joe Biden gilt nicht als großer Facebook-Fan. Donald Trump wütete zwar gegen das Silicon Valley, handelte aber nur selten. Das könnte sich unter Biden ändern. Für Nutzerinnen und Nutzer sind die Änderungen dagegen auf jeden Fall eine gute Nachricht. Sie können sich mit einem Klick ein Stück ihrer Privatsphäre zurückholen. Und wer lieber personalisierte Werbung sieht, kann dem Tracking ja zustimmen (Hurtz, Die große Angst vor einem kleinen Pop-up, SZ 28.12.2020, 18; Martin-Jung, Facebooks neuer Erzfeind, SZ 29.01.2021, 23).

EU-weltweit

Geheimdienste kooperieren zwecks Brechen von Verschlüsselung

Aus Dokumenten der deutschen EU-Ratspräsidentschaft, die bis Ende 2020 dauerte, an die Mitgliedsstaaten geht hervor, dass die EU-Staaten künftig enger mit der angelsächsischen Geheimdienstallianz der „Five Eyes" zusammenarbeiten wollen, um sichere Verschlüsselung in digitaler Kommunikation zu umgehen. Als „Five Eyes" kooperieren die Geheimdienste der USA, Großbritanniens, Australiens, Neuseelands und Kanadas miteinander.

Die Formulierungen im Entwurf eines EU-Papiers entsprechen denen einer Erklärung der Geheimdienstallianz „Five Eyes" sowie Indiens und Japans vom 11.10.2020, wobei jeweils der „rechtmäßige Zugriff auf verschlüsselte Kommunikation" gefordert wird. Ein weiteres Papier aus dem EU-Ministerrat vom 16.11.2020 erhärtet den Verdacht eines abgestimmten Vorgehens: Das Dokument namens „Empfehlungen für den künftigen Umgang mit dem Thema Verschlüsselung" richtet sich an die EU-Mitgliedsstaaten und ist eine Art Handreichung. Unter Punkt sechs ist zu lesen, die Regierungen sollten sich zu dem Thema eng mit den Initiatoren des Papiers „End-to-End-Encryption and Public Safety" austauschen. Das ist jene Erklärung der Five-Eyes-Länder sowie Indiens und Japans, in der sie Unter-

nehmen wie Facebook auffordern, Staaten Zugang zu verschlüsselten Inhalten zu ermöglichen.

Bis 2013 konnte die Five-Eyes-Allianz einen guten Teil der weltweiten Kommunikation abhören. Als dann der ehemalige NSA-Mitarbeiter Edward Snowden die Abhörpraktiken enthüllt hatte, fingen viele Anbieter von Messaging-Apps an, sich ernsthaft über den Schutz privater Kommunikation Gedanken zu machen. Sieben Jahre später ist sichere Verschlüsselung bei WhatsApp, Signal und anderen Messengern Standard. Zuletzt wurde bekannt, dass auch Google Endezu-Ende-Verschlüsselung (E2EE) in den RCS-Standard einbauen will, der Nachfolger der SMS werden soll. Dies ärgert Geheimdienste und Strafverfolgungsbehörden weltweit. Deshalb drängen sie auf technische Lösungen, die ihnen den Zugriff auf die Kommunikation von Verdächtigen wieder ermöglichen würden.

Dabei helfen, so das Statement der „Five Eyes" wie auch die Papiere der EU, soll eine Allianz aus Telekom-Anbietern, Tech-Unternehmen und Behörden. Unklar ist jedoch, wie das gelingen soll ohne die Verschlüsselung insgesamt unbrauchbar zu machen. Experten betonen seit Jahren, dass es E2EE nur ganz oder gar nicht gibt. Bei der Methode werden Nachrichten am Anfang der Kommunikation auf dem Gerät des Senders verschlüsselt. Erst am anderen Ende, auf dem Gerät des Empfängers, wird die Nachricht wieder entschlüsselt. Selbst wenn die Verantwortlichen bei WhatsApp, Signal oder etwa der Telekom etwas anderes wollten: Sie haben nur Zugriff auf einen Buchstabensalat. Sie bleiben bloße Überbringer einer Nachricht, die sie nicht lesen können.

Ermittler müssen sich deshalb aktuell direkten Zugriff auf ein Handy oder einen Computer verschaffen, um Nachrichten zu lesen, die mit einem solchen Verfahren verschickt werden. Viele Sicherheitspolitiker wünschen sich, die Unternehmen würden sogenannte Hintertüren in ihren Programmcode einbauen, durch die Behörden Zugriff auf unverschlüsselte Daten erhalten. Doch solche gezielt eingebauten Schwachstellen könnten auch Kriminelle und alle anderen Geheimdienste ausnutzen.

Wie heikel das Thema Verschlüsselung ist, war offensichtlich auch der deutschen EU-Ratspräsidentschaft bewusst. In einer „Entschließung des Rates zu Verschlüsselung" eines vorbereitenden Ausschusses der EU wird einerseits sichere Verschlüsselung als wichtige Errungenschaft gelobt. Zugleich fordert diese die Mitgliedsstaaten aber auf, Lösungen zu suchen, mit denen Sicherheitsbehörden trotz Verschlüsselung „rechtmäßig und gezielt auf Daten zugreifen" können (dazu siehe oben S. 26).

Ein Gesetz, um Verschlüsselung grundsätzlich zu schwächen, könnte nur die EU-Kommission vorschlagen. Die zuständige Innenkommissarin Ylva Johansson sagte Mitte November 2020 im Parlaments-Ausschuss für bürgerliche Freiheiten, sie suche nach Möglichkeiten die Sicherheit der Verschlüsselung zu wahren, Strafverfolgungsbehörden aber gleichzeitig effektive Mittel für ihre Ermittlungen an die Hand zu geben. Das EU-Parlament müsste über ein solches Gesetz mitentscheiden. Fachpolitiker aus den Fraktionen der Sozialdemokraten, der Grünen und der Liberalen hatten bereits nach Bekanntwerden der ersten Berichte vor Versuchen gewarnt Endezu-Ende-Verschlüsselung aufzuweichen (Muth, Allianz gegen verschlüsselte Nachrichten, SZ 30.11.2020, 9).

EU

Standardvertragsklauseln werden überarbeitet

Nachdem der Europäische Gerichtshof (EuGH) im Juli 2020 den transatlantischen „Privacy Shield" und damit eine der wichtigsten Grundlagen für den Transfer von personenbezogenen Daten aus der EU in die USA für ungültig erklärt hat versucht die EU-Kommission nun ein prinzipiell verbliebenes alternatives Instrument zu retten und legte am 13.11.2020 einen Entwurf für neue sogenannte Standardvertragsklauseln (SVK) für die Informationsweitergabe in Drittstaaten, etwa die USA, vor. Die überarbeiteten SVK sollen nach Angaben der Brüsseler Regierungsinstitution die Vorgaben aus dem „Schrems-II-Urteil" des EuGH (DANA 3/2020, 199 ff.) sowie neue Empfehlungen des Europäischen Datenschutzausschusses (EDSA) dazu berücksichtigen.

Der EuGH hatte im Schrems-II-Urteil zum wiederholten Mal festgestellt, dass US-Gesetze wie der FISA oder der Cloud Act eine Massenüberwachung durch Sicherheitsbehörden wie die NSA oder das FBI ermöglichten und der Datenschutzstandard daher nicht dem in der EU entspricht. In dem Vorschlag der Kommission heißt es nun, dass die Klauseln – „insbesondere im Lichte der Rechtsprechung des Gerichtshofs" – besondere Garantien vorsehen sollten, „um etwaige Auswirkungen der Gesetze des Bestimmungsdrittlands" auf die Einhaltbarkeit der SVK durch den Datenimporteur zu regeln. Dabei gelte es vor allem zu klären „wie mit verbindlichen Ersuchen von Behörden im Drittland nach einer Weitergabe der übermittelten personenbezogenen Daten umzugehen ist".

Der Transfer und die Verarbeitung persönlicher Informationen sollten dem Entwurf zufolge nur dann erfolgen, „wenn die Gesetze des Bestimmungsdrittlandes den Datenimporteur nicht daran hindern diese Klauseln einzuhalten". Sei es nötig Übermittlungen in Drittländer zu stoppen, da die SVK nicht eingehalten werden könnten, unterrichte der zuständige Mitgliedsstaat unverzüglich die Kommission. Diese werde die entsprechende Botschaft an die anderen EU-Länder weiterleiten.

Details zu den Auflagen, die im SVK-Entwurf schon anklingen, sind in einem Anhang vorgesehen: Die Vertragsparteien sollen demnach gewährleisten keinen Grund zu der Annahme zu haben, dass die Gesetze im Bestimmungsland „einschließlich etwaiger Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die den Zugang von Behörden ermöglichen, den Datenimporteur an der Erfüllung seiner Verpflichtungen aus diesen Klauseln hindern". Dies beruhe auf dem Verständnis, dass Gesetze, die das Wesen der Grundrechte und -freiheiten respektierten und in einer demokratischen Gesellschaft notwendig und verhältnismäßig seien, nicht im Widerspruch zu den Klauseln stünden. Der Importeur erklärt sich mit dem Zusatz zudem bereit Betroffene unverzüglich zu benachrichtigen, wenn er einen rechtsverbindlichen Antrag einer Behörde auf eine Daten-

herausgabe erhält. Mitzuteilen seien dabei Details zu den angeforderten personenbezogenen Informationen, das anfordernde Amt, die Rechtsgrundlage für den Antrag und die erteilte Antwort.

Wenn es dem Datenbezieher untersagt ist den Lieferanten oder die direkten Betroffenen zu benachrichtigen, muss er sich „nach besten Kräften um eine Aufhebung des Verbots“ bemühen, „um so viele Informationen wie möglich und so bald wie möglich zu übermitteln“. Zudem soll der Importeur gegebenenfalls „alle verfügbaren Rechtsmittel zur Anfechtung des Antrags“ ausschöpfen. Zeitgleich müsse er sich um einstweilige Maßnahmen bemühen, „um die Wirkungen des Ersuchens auszusetzen, bis das Gericht in der Sache entschieden hat“. Anzugeben sind zudem getroffene Maßnahmen, mit denen die Menge der persönlichen Daten vor einem Transfer möglichst gering gehalten, pseudonymisiert und verschlüsselt wird. Wenn die Verarbeitung über einen externen Dienstleister läuft, müssen die Lieferanten sicherstellen, dass auch dieser die nötigen zusätzlichen Vorkehrungen trifft.

Die im EDSA versammelten Datenschutzbehörden führen in ihren Ratschlägen zur Umsetzung des Schrems-II-Urteils parallel auf Basis einer früheren Frage-Antwort-Liste aus, dass die Verantwortlichen beim Transfer persönlicher Informationen insbesondere in die USA „zusätzliche Maßnahmen“ treffen müssten. Damit sei „das gleiche Datenschutzniveau“ wie in der EU zu gewährleisten. Die genauen Umstände von Übertragungen müssten „von Fall zu Fall“ betrachtet werden. Dies gelte für Transfers in alle Drittstaaten.

Zudem hat die Kommission einen Entwurf für Muster-Datenschutzklauseln zwischen Firmen oder Behörden und Auftragsarbeitern vorgelegt, die ihren Sitz in der EU haben. Zu beiden Initiativen wurde Ende 2020 eine öffentliche Konsultation durchgeführt. Die Schlussklauseln will die Brüsseler Exekutivinstanz im Anschluss veröffentlichen, wenn von den Mitgliedsstaaten kein Widerspruch kommt (Krempl, US-Datentransfer: EU-Kommission schlägt neue Standardvertragsklauseln vor, www.heise.de 14.11.2020; Kurzlink: https://heise.de/-4960486).

EU

Druck auf irische Datenschutzaufsicht DPC in Sachen „Facebook“

Im dem beim Europäischen Gerichtshof (EuGH) laufenden Verfahren zwischen belgischer Datenschutzbehörde und Facebook hat der EuGH-Generalanwalt Michal Bobek eine Stellungnahme abgegeben zu der für die Auslegung der Datenschutz-Grundverordnung (DSGVO) wichtigen Frage, ob nationale Datenschutzbehörden agieren dürfen, auch wenn eine andere Behörde federführend ist. Darin heißt es: „Die anderen betroffenen nationalen Datenschutzbehörden seien gleichwohl befugt, in Situationen, in denen es ihnen die Datenschutz-Grundverordnung spezifisch gestatte derartige Verfahren in ihren jeweiligen Mitgliedsstaaten einzuleiten.“

Die belgische Datenschutzbehörde will gegen Facebook vorgehen, obwohl wegen der Hauptniederlassung in Irland die dortige Behörde (Data Protection Commissioner – DPC) zuständig ist. Bereits 2015, also noch vor Inkrafttreten der DSGVO, hatte sie vor belgischen Gerichten ein Verfahren gegen Facebook laufen, in dem es um die Weitergabe der Daten in die USA ging. Nachdem ein Gericht entschied, die DPC sei zuständig, liegt das Verfahren nun bei einem Berufungsgericht. Dieses möchte nun vom EuGH wissen, ob nur die DPC oder auch nationale Datenschutzbehörden handeln dürfen.

Gemäß Bobek hat die federführende Datenschutzbehörde zwar eine allgemeine Zuständigkeit und haben andere Behörden dadurch weniger umfassende Handlungsbefugnisse. Dennoch gibt es dem Generalanwalt nach im Sinne der DSGVO Ausnahmen, wenn bei Dringlichkeit Maßnahmen ergriffen werden müssen oder sie tätig würden, „nachdem die federführende Datenschutzbehörde beschlossen habe sich nicht selbst mit dem Fall zu befassen.“ Diese Einschätzung ist ein Entscheidungsvorschlag an den EuGH der zu einem späteren Zeitpunkt die Entscheidung zu treffen hat.

Die DPC kündigte just darauf an in der Sache Max Schrems versus Facebook eine Entscheidung zu treffen. Diese steht seit mehr als sieben Jahren aus. Nicht nur der gegen den DPC klagende Datenschutzaktivist Schrems und sein Verein noyb („none of your business“) kritisieren den DPC wegen Verzögerungen. Eine Entscheidung des EuGH im Sinne des Generalanwalts könnte bedeuten, dass in einem solchen Fall auch andere nationale Datenschutzbehörden Entscheidungen treffen können. Gemäß noyb wird in seinem Verfahren auf Basis der DSGVO entschieden, obwohl diese bei Einreichung der Klage noch nicht in Kraft getreten war: „Im Rahmen der DSGVO hat die DPC das Recht, eine Geldstrafe in Höhe von bis zu 4 Prozent des weltweiten Umsatzes von Facebook und Verbote zur Datenverarbeitung zu verhängen.“ Die Entscheidung könne das ursprüngliche Beschwerdeverfahren von 2013 zu dem Fall machen, der endgültig das Schicksal von Facebooks EU-US-Datentransfer besiegelt. Schrems erwartet, dass die Verfahrenskosten von der DPC zu tragen seien. In den vergangenen sieben Jahren lag der Fall inzwischen bei sieben Gerichten: „Mehrere Gerichte haben entschieden, dass die DPC der Beschwerde nachgehen muss.“ Es gab jedoch zahlreiche Nebenschauplätze und Pausen.

Der EuGH hat im Juli 2020 das Privacy-Shield-Abkommen gekippt, was dazu führte, dass damit die rechtliche Grundlage für die Datenübertragung in die USA fehlt (DANA 3/2020, 199 ff.). Facebook, wie auch andere Unternehmen, beriefen sich auf Standardvertragsklauseln, die ein gleichwertiges Datenschutzniveau herstellen sollen, so dass der Transfer in Drittländer erlaubt ist. Die DPC verhängte eine Anordnung, dass Facebook daher die Datenübertragung stoppen müsse, das Datenschutzniveau sei nicht gleichwertig. Facebook drohte im Gegenzug damit, seine Dienste in der EU einzustellen, und reichte Beschwerde beim irischen High Court ein. Diese wird damit begründet, dass das Verfahren um den Datentransfer nicht abgeschlossen sei. Der High Court entschied, es müsse eine gerichtliche Überprüfung geben.

Schrems wird nun angehört und bekommt Einsicht in alle von Facebook eingereichten Unterlagen. Nach der Entscheidung aus dem Sommer 2020 hatte die DPC zur Klärung der Rechtslage eine

Klage gegen Schrems und Facebook eingereicht und das eigentliche Verfahren von 2013 auf unbestimmte Zeit pausiert. Beide Parteien klagten ihrerseits, wobei Facebook zurückzog, Schrems jedoch auf einer Entscheidung bestand, die nun folgen dürfte (Weiß, EuGH-Generalanwalt empfiehlt: Nationale Datenschutzbehörden dürfen eingreifen, www.heise.de 14.01.2021, Kurzlink: https://heise.de/-5024130; Weiß, Entscheidung angekündigt: Schrems versus Facebook versus irische Datenbehörde, www.heise.de 14.01.2021, Kurzlink: https://heise.de/-5023827).

EU

Automatisiertes Kindesmissbrauchs-Inhaltsscanning soll erlaubt werden

Anbieter internetbasierter E-Mail- und Messaging-Dienste wie Facebook oder Google mit Gmail sollen nach wie vor sämtliche private Nutzernachrichten ohne Anlass und Verdacht auf Darstellungen sexuellen Kindesmissbrauchs hin scannen dürfen. Auf einen entsprechenden Verordnungsentwurf haben sich die Botschafter der EU-Mitgliedstaaten am 28.10.2020 geeinigt. Sie erteilten der deutschen Ratspräsidentschaft ein Mandat, über die geplante Vorschrift mit der EU-Kommission und dem Parlament zu verhandeln.

Die bis Ende 2025 befristete Verordnung halten die EU-Länder für nötig, da vom 21.12.2020 an der europäische Kodex für die elektronische Kommunikation greift. Damit fallen „nummernunabhängige interpersonelle Kommunikationsdienste“ wie Webmail und Messaging, für die bisher die Datenschutz-Grundverordnung (DSGVO) galt, in den Anwendungsbereich der E-Privacy-Richtlinie (Telekommunikations-Datenschutz-Richtlinie). Diese enthält im Gegensatz zur DSGVO keine ausdrückliche Rechtsgrundlage für die freiwillige Verarbeitung von Inhalten oder Verbindungs- und Standortdaten, um sexuelle Missbrauchsdarstellungen ausfindig zu machen.

Die Kommission brachte daher im September eine Übergangsverordnung mit einer Ausnahme von der E-Privacy-Richtlinie ins Spiel, damit einschlägige Anbieter ihre laufenden Aktivitäten zur Suche nach solchen illegalen Inhalten sowie gegen das Heranpirschen von Nutzern an Kinder und Jugendliche (Cybergrooming) fortsetzen können. Voraussetzung dafür ist, dass die Maßnahmen mit der DSGVO im Einklang stehen.

Der Ministerrat unterstützt diesen Kurs mit seiner Position prinzipiell, setzt aber laut dem Beschluss im Ausschuss der Ständigen Vertreter der Mitgliedstaaten (Coreper) noch auf Verschärfungen. So soll etwa eine Einschränkung gestrichen werden, wonach die Dienstleister Nachrichten nicht „systematisch filtern“ und scannen, sondern nur bei konkretem Verdacht in spezifische Kommunikation schauen dürften. Meldet ein Algorithmus einen Verdachtsfall, dürfen Inhalt einer Botschaft sowie Nutzerdaten dem Plan nach automatisiert und ohne menschliche Prüfung an Strafverfolgungsbehörden und Nichtregierungsorganisationen weltweit weitergeleitet werden. Die Betroffenen sollen davon nichts erfahren.

Die Kommission kündigte an bis zum zweiten Quartal 2021 Rechtsvorschriften zur Bekämpfung des sexuellen Missbrauchs von Kindern im Internet vorzuschlagen. Mit diesen Rechtsvorschriften soll eine langfristige Lösung geboten werden, um die befristeten Vorschriften zu ersetzen. Der Europäische Datenschutzausschuss (EDSA) wird dem Entwurf nach aufgefordert Richtlinien für einschlägige Suchmaßnahmen aufzustellen. Die Kommission hat zudem bereits angekündigt bis zum zweiten Quartal 2021 umfassendere und dauerhafte Rechtsvorschriften im Kampf gegen sexuellen Missbrauchs von Kindern im Internet vorzuschlagen. Diese sollen die befristete Verordnung ersetzen und eine Lösung für das von der Brüsseler Regierungsinstitution ausgemachte Problem der Ende-zu-Ende-Verschlüsselung enthalten: Anbieter wie WhatsApp, Signal oder Threema, die auf diesen durchgehenden Kryptographieansatz bauen, können rein technisch Nutzernachrichten nicht auf illegale Inhalte hin durchsuchen.

Der für die Piraten im EU-Parlament sitzende Abgeordnete Patrick Breyer aus Schleswig-Holstein hat derweil beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) Beschwerde gegen die Praktiken von Facebook & Co. eingelegt: „Die Totaldurchleuchtung unserer privaten Kommunikation bei US-Anbietern kann dazu führen, dass deren Algorithmen private und intime Bilder über unsere Gesundheit oder Sexualität fälschlich melden und die zuständigen Mitarbeiter sie illegal weiter verbreiten. Da Jugendliche nicht selten intime Fotos untereinander teilen, könnten Konzernmitarbeiter sogar zusätzliche ‚Kinderpornografie‘ in Umlauf bringen.“ Dieser „Zensursula-Plan“ gefährde „Sicherheit und Privatsphäre von Kindern und Erwachsenen gleichermaßen und gehört gestoppt“. Auch die Weitergabe „vermeintlicher Treffer“ an das National Center for Missing & Exploited Children (NCMEC) in den USA verstoße gegen die DSGVO. Gerade erst habe der Europäische Gerichtshof entschieden, dass eine automatisierte Kommunikationsanalyse allenfalls bei akuter Bedrohung der nationalen Sicherheit verhältnismäßig sein könne (Krempl, EU-Rat: Facebook & Co. können weiter nach Kinderpornografie suchen, www.heise.de 29.10.2020, Kurzlink: https://heise.de/-4943055).

EU

Kritik an geringem EDSA-Bußgeld gegen Twitter

Am 16.12.2020 verkündete die irische Datenschutzbehörde, die Data Protection Commission (DPC), dass sie ihren ersten „Big Tech“-Fall abgeschlossen und damit zugleich das erste Streitschlichtungsverfahren nach Artikel 65 der Datenschutz-Grundverordnung (DSGVO) durchlaufen hat: Twitter muss nach einer zu spät gemeldeten Datenpanne, die mindestens 88.726 Nutzer in der EU zwischen September 2017 und Anfang 2019 betroffen haben soll, 450.000 Euro Bußgeld zahlen.

Im Vergleich zu den Sanktionen, die die französische Datenschutzbehörde CNIL bereits mit einer Buße von bis zu 100 Mio. € gegen Google in nationalen Fällen verhängte, nimmt sich der Betrag sehr gering aus. Das von Twitter selbst als „signifikant“ eingestufte Leck

entstand durch einen Fehler im Design des Kurznachrichtendienstes. Wenn ein Nutzer auf einem Android-Gerät die mit seinem Konto verknüpfte E-Mail-Adresse änderte, waren die geschützten Tweets ungeschützt und so für eine breitere Öffentlichkeit zugänglich, nicht nur für seine Follower.

Ein externer Auftragnehmer hatte das Problem am 26.12.2018 im Rahmen des Bug-Bounty-Programms von Twitter entdeckt, über das jeder einen Fehlerbericht einreichen kann. Während der daraufhin eingeleiteten Untersuchung entdeckte Twitter weitere Benutzeraktionen, die ebenfalls zu demselben unbeabsichtigten Ergebnis führten. Den Fehler führte der Konzern auf eine Codeänderung vom 04.11.2014 zurück. Potenziell Betroffene konnte er aber nur bis 2017 zurückverfolgen, da für die restlichen drei Jahre keine Logfiles mehr vorlagen.

Das Rechtsteam von Twitter erfuhr von dem Bug am 02.01.2019. Am 08.01.2019 informierte der Konzern, der – wie viele andere US-Internetriesen – seinen europäischen Hauptsitz in Irland hat, die DPC. Rechtlich ist eine Meldefrist von 72 Stunden vorgesehen. Anderthalb Jahre später legte die Datenschutzbehörde nach Ende ihrer Untersuchungen und Abstimmungsrunden mit Twitter den Entwurf für ihre Entscheidung dem Europäischen Datenschutzausschuss (EDSA) vor. Kontrolleure aus acht Mitgliedsstaaten inklusive Deutschlands brachten dagegen Bedenken vor. Anfang November war das Schlichtungsverfahren beendet. Den entsprechenden Beschluss hat der EDSA nun öffentlich gemacht.

Der Hamburgische Datenschutzbeauftragte Johannes Caspar, der den Fall für Deutschland betreut, ist mit der Entscheidung im Artikel-65-Verfahren alles andere als zufrieden. Diese führe dazu, „dass die federführende Behörde künftig den Untersuchungsbereich von Verstößen gegen die DSGVO selbst bestimmen kann“. Damit „entmachtet sich“ der EDSA und gebe eine eigenständige Kontrolle der federführenden nationalen Prüfer aus der Hand. Die DPC habe nur den Verstoß gegen die Meldepflicht nach Artikel 33 DSGVO beleuchtet, kritisiert Caspar. So seien „weitergehende dahinterliegende Fragen“ außen vor geblieben. Mögliche Verstöße etwa gegen Integrität, Vertraulichkeit und Sicherheit der Datenverarbeitung hätten gar keine Rolle gespielt. Dies gelte auch für eine potenzielle gemeinsame Verantwortung mit Blick auf die Twitter-Konzernzentrale in den USA.

Caspar kritisiert: „Ist dies der Maßstab, mit dem künftig Entscheidungen im Streitbeilegungsverfahren durch den EDSA überprüft werden, bleibt eine einheitliche Anwendung der DSGVO in der EU auf der Strecke. Es liegt dann bei der federführenden Behörde, zusammenhängende Sachverhalte so zu verkürzen und einzudampfen, dass es eigentlich keines gemeinsamen Verfahrens auf EU-Ebene mehr bedarf. Die Höhe des Bußgeldes ist eine zentrale Fragestellung, die in der EU die Einheitlichkeit des Vollzugs wesentlich beeinflusst“. Der Beschluss der DPC liege auf der „bereits seit langem problematischen Linie einer Zweispurigkeit des Datenschutzes in Europa“: Während in den nationalen Verfahren der Bußgeldrahmen der DS-GVO zusehends ausgeschöpft werde, hätten die bislang spärlich verhängten Sanktionen bei der grenzüberschreitenden Datenverarbeitung „bestenfalls einen symbolischen Wert“. Die erforderliche Abschreckung „wird so jedenfalls nicht hergestellt“.

Im Ergebnis privilegiere dies „globale Tech-Firmen, die sich in einigen Mitgliedstaaten niedergelassen haben, und führt zu Wettbewerbsverzerrungen auf dem digitalen Markt nicht zuletzt zu Lasten von Unternehmen in anderen Mitgliedstaaten“. Leider habe die EU-Kommission auch im gerade vorgestellten Digital Services Act (DSA) hierzu keine Antworten gegeben. Wenn es nicht gelinge, nötige Veränderungen herbeizuführen, bleibe eine eigenständige Digitalpolitik in der EU im Bereich der Wunschvorstellung.

Die Hamburgische Datenschutzbehörde prüft, ob sie Rechtsmittel vor dem Europäischen Gerichtshof gegen die Entscheidung des EDSA einlegen soll. Klar ist für Caspar schon jetzt, dass dessen erste Entscheidung im Mediationsprozess „nicht der Maßstab für sein künftiges Handeln werden“ dürfe.

Der Bundesdatenschutzbeauftragte Ulrich Kelber, Caspar und einige ihrer Kollegen versuchen seit Längerem, die Iren auch bei Facebook&Co. zum Jagen zu tragen. Die DPC gilt als chronisch unterbesetzt sowie voreingenommen und kommt in den von ihr eingeleiteten großen internationalen Verfahren nur langsam voran. Der EDSA hatte im Februar 2020 gefordert, dass die Zusammenarbeit in diesem Bereich dringend verbessert werden müsse. 2021 erhält die DPC zwar 2,2 Millionen mehr Budget. Berichten zufolge hatte sie aber ein Plus von knapp sechs Millionen Euro gefordert (Krempl, Kleine DSGVO-Strafe: EU-Datenschützer entmachten sich im Fall Twitter, www.heise.de 19.12.2020, Kurzlink: https://heise.de/-4995833).

EU

Künftig Verbands-Sammelklagen in den EU-Mitgliedsstaaten

Das Europaparlament nahm am 25.11.2020 eine Initiative zur Einführung von Sammelklagen in den 27 EU-Staaten an. Demgemäß sollen Verbraucher ihre Rechte gegenüber großen Firmen leichter durchsetzen können. Bestimmte Institutionen wie Verbraucherverbände können dann stellvertretend für die Geschädigten gegen Unternehmen auf Unterlassung und Schadenersatz klagen. Die EU-Länder haben zwei Jahre Zeit ihre Gesetzgebung entsprechend anzupassen.

Entschädigungen sind so etwa in den Bereichen Datenschutz, Finanzdienstleistungen, Gesundheit und Flug- und Bahnverkehr möglich. EU-Justizkommissar Didier Reynders sagte angesichts der vielen ausgefallenen Flüge im Jahr 2020, diese Verbandsklagen seien jetzt notwendiger denn je. Die Sammelklagen lieferten soliden Schutz für Verbraucher.

Der CDU-Abgeordnete Andreas Schwab monierte hingegen fehlende Einheitlichkeit bei der Ausgestaltung der Klagemöglichkeit in den einzelnen EU-Ländern. Reynders zufolge gibt es in einigen Staaten bereits gut funktionierende Regelungen zu Verbandsklagen. Diese sollten beibehalten werden. Die Sozialdemokratin Lara Wolters mahnte an, dass Verbandsklagen nicht nur für Verbraucher und nicht nur für EU-Bürger zur Verfügung stehen sollten.

Hintergrund der Regelung sind Fälle wie manipulierte Abschalteinrichtungen mit Hunderttausenden Geschädigten. Jeder Einzelne für sich hat nur geringe Chancen – allein deshalb, weil ihm womöglich die Ressourcen für einen Rechtsstreit gegen Großunternehmen fehlen. Anders sieht es aus, wenn Verbraucher sich zusammenschließen und gemeinsam klagen können. Deshalb schlug die EU-Kommission 2018 vor europaweit Kollektivklagen zu erlauben. Nach Angaben der Kommission gibt es bereits in 19 Mitgliedstaaten kollektive Rechtsbehelfe, auch in Deutschland. Mit den neuen EU-Regeln müssten Verbraucher ihren Schadenersatz nicht mehr individuell einklagen. Zudem könnten sie künftig auch in anderen EU-Staaten ihre Rechte durchsetzen (Europaparlament macht Weg für Verbandsklagen frei, www.proplanta.de 25.11.2020).

Frankreich

Hohe Bußgelder gegen Google und Amazon wegen Cookies

Die französische Datenschutzaufsicht will mit hohen Zwangsgeldern Google und Amazon dazu bringen ihre Cookie-Politik zu ändern. Die Commission Nationale de l'Informatique et des Libertés (CNIL) teilte am 10.12.2020 mit, dass gegen Google 100 Mio. € und gegen Amazon 35 Mio. € festgelegt worden sind. In den Verfahren geht es um Cookies, die nach Überzeugung der Behörde dem Werbetargeting dienen. Die CNIL bemängelt, dass auf den französischen Portalen von Google und Amazon Werbecookies gesetzt wurden, bevor die Nutzer explizit ihre Zustimmung erteilt hatten.

Im Fall von Google wurde zwar ein Cookie-Dialog angezeigt, der Nutzern die Wahl ließ die Datenschutzeinstellungen aufzurufen oder direkt auf das Angebot zuzugreifen. Nach Auffassung der Datenaufsicht reichte dies jedoch nicht aus eine tatsächlich informierte Einwilligung zum Setzen von Werbe-Cookies zu erhalten. Zudem sei auch bei Nutzern, die der personalisierten Werbung ausdrücklich widersprochen hätten, immer noch ein Werbecookie gesetzt worden. Zwar hatte Google bei einem Seiten-Update im September 2020 aufgehört ungefragt Werbecookies zu setzen. Die seither angebotenen Informationen reichten aber immer noch nicht aus, um Nutzer darüber aufzuklären, welche Informationen verarbeitet werden und dass sie der Cookie-Speicherung auch widersprechen können. Weil die Speicherung 50 Millionen Internetnutzer in Frankreich betreffe und das Werbegeschäft von Google so weitreichende Konsequenzen habe, wurde Google LLC ein Bußgeld von 60 Millionen Euro, der Europazentrale in Irland zusätzlich 40 Millionen Euro Strafe auferlegt.

Die Vorwürfe gegen Amazon sind ähnlich. So hat auch Amazon laut Darstellung der Behörde im September 2020 ein verbessertes Cookie-Banner eingerichtet. Dieses informiere die Nutzer aber immer noch nicht ausreichend. Die Höhe des Bußgeldes begründet die CNIL mit der Bedeutung von Amazon für den E-Commerce in Frankreich und dem Werbegeschäft, bei dem einmal angesehene Artikel auch auf anderen Websites beworben werden.

Die Unternehmen haben drei Monate Zeit, um ihre Angebote nach den Vorgaben der Datenschützer anzupassen. Sollte dies nicht geschehen, droht die CNIL mit weiteren Strafzahlungen von 100.000 Euro für jeden weiteren Tag Verzögerung. Beide Unternehmen zeigten sich über das Vorgehen der CNIL verärgert. So verwies Google auf die unsichere Rechtslage und will sich um weitere Gespräche mit der Datenschutzaufsicht bemühen. Amazon betonte die Privatsphäre seiner Kunden bestmöglich zu schützen.

Eigentlich gilt in Europa nach der Datenschutz-Grundverordnung (DSGVO) ein „One Stop Shop"-Prinzip, wonach letztlich nur eine Datenschutzbehörde für die Unternehmen zuständig ist. Im Fall von Google wäre das Irland. Die dortige Aufsichtsbehörde wird seit Jahren von europäischen Kollegen wegen Untätigkeit kritisiert. Deshalb berief sich die französische CNIL auf eine andere Rechtsgrundlage: Die europäische E-Privacy-Richtlinie wurde bereits vor der DSGVO in französisches Recht umgesetzt. Der Versuch der Harmonisierung zu einer neuen E-Privacy-Verordnung war jedoch bisher immer wieder an der Uneinigkeit europäischer Regierungen gescheitert, sodass die alten Vorschriften weiterhin gelten. Die CNIL ist eine der europäischen Behörden, die den meisten Druck machen bei der Umsetzung des Datenschutzes. So hatte die CNIL bereits 2019 eine Strafe von 50 Millionen Euro gegen Google verhängt, die trotz rechtlicher Gegenwehr des Konzerns aufrechterhalten wurde (Kleintz, Frankreich: Datenschützer verhängen Millionen-Bußgelder gegen Google und Amazon, www.heise.de 10.12.2020, Kurzlink: https://heise.de/-4985956).

Frankreich

DSGVO-Millionenbußgeld gegen Carrefour

Der französische Einzel- und Großhandelsriese Carrefour hat wegen mehrerer Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) eine Geldbuße in Höhe von insgesamt 3,05 Mio. € auferlegt bekommen. Der Vorwurf besteht in der Verletzung von Lösch- und Informationspflichten. Die nationale Datenschutzbehörde CNIL hatte mehrfache Beschwerden gegen die Gruppe erhalten und zwischen Mai und Juli 2019 Inspektionen vor Ort durchgeführt. Eine Forderung von 2,25 Millionen € ging an den Mutterkonzern, die Banktochter Carrefour Banque soll 800.000 € bezahlen.

Die CNIL-Prüfer hatten u.a. festgestellt, dass der französische Marktführer die Daten von mehr als achtundzwanzig Millionen früheren Kunden im Rahmen eines Bonusprogramms gespeichert hatte, obwohl diese seit fünf bis zehn Jahren inaktiv waren. Dasselbe galt für 750.000 Nutzer der Website carrefour.fr. Die praktizierte Aufbewahrungsfrist von vier Jahren für Kundendaten nach dem letzten Kauf sei überschritten worden.

Carrefour hat der CNIL zufolge zudem gegen Informationspflichten aus der DSGVO verstoßen. Die Angaben, die das Unternehmen den Besuchern der Stammwebseite und von carrefour-banque.fr sowie den Inhabern der Bonuskarte zur Verfügung stellte, seien schwer zugänglich, kaum verständlich und lückenhaft gewesen. Ferner seien Cookies ohne die erforderliche Einwilligung gesetzt worden. Carrefour habe ungerechtfertigt einen Identitätsnachweis verlangt, wenn Kunden ihre ver-

brieften Kontrollrechte ausüben wollten. Auskunftsersuchen sei der Konzern zu spät oder gar nicht nachgekommen. Für das Treueprogramm habe das Unternehmen persönliche Kontaktangaben erhoben und – entgegen der Zusage – an den hauseigenen Finanzdienstleister weitergegeben. Von weiteren und schärferen Sanktionen sah die CNIL ab, da Carrefour „erhebliche Anstrengungen unternommen" habe, um alle festgestellten Verstöße zu beheben (Krempl, DSGVO-Verstöße: Über drei Millionen Euro Strafe für Carrefour, www.heise.de 26.11.2020, Kurzlink: https://heise.de/-4972448).

Frankreich

Gesetzentwurf zielt auf Bilderzensur in den Medien ab

In Frankreich soll ein Gesetz verbieten Polizisten im Einsatz zu fotografieren und zu filmen. Zeitungen, Rundfunk- und Fernsehanstalten befürchten als Nebeneffekt eine Einschränkung der kritischen Berichterstattung über unangemessene Polizeieinsätze. Im Mittelpunkt der Diskussion des von der Regierungspartei La République en Marche eingebrachten Gesetzes steht der Artikel 24. Dieser sieht vor, dass die Verbreitung von Bildern über Polizeiaktionen mit erkennbarem Gesicht der Sicherheitskräfte mit Gefängnis und bis zu 45.000 Euro Bußgeld bestraft werden kann, sofern die klare Absicht dahinterstehe den Polizisten „physisch oder psychisch zu schaden".

So war Anfang November 2020 auf Instagram ein Polizist bei einer Schülerblockade in Paris zu sehen, der einem Journalisten Pfefferspray in Gesicht und Kamera sprühte, während ein anderer seinem Kollegen im Streifenwagen zurief: „Komm, überfahr ihn doch." Diese Szene, die zu vielen Aufrufen und Kommentaren führte, könnte nach der geplanten Gesetzesänderung zur „globalen Sicherheit" in den französischen Netzwerken künftig verboten sein.

Die Regierung will mit dieser Initiative auf die seit der Gelbwestenbewegung wachsende Spannung zwischen der Polizei und einem Teil der Bevölkerung eingehen. Hasstiraden gegen manchmal namentlich genannte Polizisten auf den sozialen Medien führen zu Verstimmung auf den Polizeirevieren. Die Polizei steht seit Monaten durch die Terrorismusgefahr, die Covid-Ausgangssperre und diverse Protestbewegungen im harten Dauereinsatz. Die Fälle von Gewalt gegen Polizisten waren in den vergangenen zwei Jahren um 18% gestiegen. 2016 hatte ein Täter aus dem Netz die Adresse eines Polizistenpaares ausfindig gemacht und dieses vor den Augen von deren Kindern kaltblütig ermordet. Mit der Gesetzesänderung versucht die Regierung dem Zulauf aus Polizeikreisen zu rechts-autoritären Gewerkschaften und Parteien das Wasser abzugraben.

Journalisten- und Redaktionsvertreter großer Zeitungen, Rundfunk- und Fernsehanstalten, darunter Le Monde, Le Figaro, Libération, Radio France und France Télévision, wiesen in Reaktion auf den Entwurf in einem gemeinsamen Aufruf darauf hin, dass wiederholte Fälle von Polizeigewalt gegenüber Demonstranten und Bürgern in den vergangenen Jahren hauptsächlich dank der Aufnahmen von Journalisten und Laien publik geworden seien. Öffentliche Polizeieinsätze zu dokumentieren, sei ein notwendiges Recht in der Demokratie. Angesichts der drohenden Strafe befürchten die Unterzeichner, dass Medien wie Privatzeugen sich bei Konfrontationen selbst zensieren und die Polizisten sich zu noch härterem Durchgreifen ermutigt fühlen könnten.

Die Regierungspartei versichert, dass die Informations- und Dokumentationsfreiheit der Presse durch die Gesetzesänderung nicht geschmälert werde, da verpixelte Bilder von Polizisten weiterhin gestattet würden. Dies ist wenig überzeugend. Gemäß Artikel 21 des Entwurfs sollen umgekehrt Aufnahmen von Überwachungskameras auf der Straße bei Polizeieinsätzen „zur Information der Öffentlichkeit" von den Behörden benutzt werden können. Ein Parlamentsabgeordneter erläuterte, es gehe darum im Krieg der Bilder die Deutungshoheit gegen die sozialen Medien zurückzugewinnen. Was als Wiederherstellung des Gleichgewichts in der Konfrontation zwischen Polizeigewalt und aggressiver Stimmungsmache im Internet angelegt sein soll, bedroht die Pressefreiheit. Sollte das Gesetz zur „globalen Sicherheit" durch beide Parlamentskammern kommen, wollen die Gegner hiergegen vor dem Verfassungsgericht klagen.

Die Proteste gegen das geplante Sicherheitsgesetz hielten über den Jahreswechsel hinweg an. Am letzten Januarwochenende 2021 fanden gemäß den Organisatoren im ganzen Land 64 Versammlungen statt, an denen sich gemäß offiziellen Angaben des Innenministeriums rund 32.770 Menschen beteiligt haben sollen, davon etwa 5050 in Paris. Dort wurden laut Staatsanwaltschaft 26 Menschen festgenommen (Hanimann, Lockdown im Krieg der Bilder, SZ 13.11.2020, 31; Gegen das Sicherheitsgesetz, SZ 01.02.2021, 6).

Italien

Bußgeld gegen Vodafone wegen unzulässiger Werbung

Die italienische Datenschutzbehörde Garante per la protezione dei dati personali (Garante) hält es für erwiesen, dass Vodafone Italien die Daten von Millionen von Nutzern widerrechtlich für „aggressives" Telemarketing verwendet hat, und hat den Netzbetreiber wegen „struktureller" Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) zu einer Strafe von 12,25 Millionen Euro verdonnert. Zudem wurde der Konzern zu diversen Schutzmaßnahmen verpflichtet.

Die Garante erhielt hunderte Beschwerden und Hinweise von Nutzern rund um unerwünschte Werbeanrufe durch Vodafone oder Firmen aus dem Vermarktungsnetzwerk des Telekommunikationsunternehmens. Im Rahmen der eingeleiteten Untersuchungen sei man in dem komplexen Fall darauf gestoßen, dass der Provider Anforderungen an die Einwilligung der Betroffenen nicht beachtet habe. Zudem habe er Schüsselprinzipien aus der DSGVO wie „Privacy by Design" und Nachvollziehbarkeit nicht befolgt.

Für die Aufsichtsbehörde war es „beunruhigend", dass aktive und potenzielle Kunden mit gefälschten oder nicht registrierten Telefonnummern zu Marketingzwecken angerufen worden seien. Vodafone untersuche diese Praxis selbst intern und scheine es mit einer

zwielichtigen Gruppe nicht autorisierter Callcenter zu tun gehabt zu haben, „die unter völliger Missachtung der Gesetzgebung zum Schutz persönlicher Daten Telemarketing-Aktivitäten durchführen“. Weitere Verstöße stellten die Kontrolleure im Umgang mit Kontaktlisten fest, die Vodafone von Geschäftspartnern und anderen Dritten ohne die erforderliche freie, informierte und ausdrückliche Zustimmung der Nutzer bezogen habe. Zudem hätten sich die Sicherheitsmaßnahmen zur Verwaltung von Kundendaten als unzureichend erwiesen (Krempl, DSGVO-Strafe: Vodafone Italien soll über 12 Millionen Euro zahlen, www.heise.de 23.11.2020, Kurzlink: https://heise.de/-4969037).

Schweden

Folksam-Versicherung stoppt illegale Datenkooperation

Die große schwedische Versicherung Folksam will digitaler werden und dafür möglichst viel darüber erfahren, was ihre Kunden online so treiben. Auf dieser Datengrundlage will die Gesellschaft passgenaue Versicherungsangebote machen. Deshalb hat Folksam Vereinbarungen mit Facebook, Google, Microsoft, Linkedin, Adobe und anderen Firmen geschlossen und ihnen Daten über eine Million eigener Kunden geliefert. Enthalten waren auch die Sozialversicherungsnummer, die in Schweden große Bedeutung im Alltag hat, und Daten über die Gewerkschaftsmitgliedschaft oder eine möglicherweise bestehende Schwangerschaftsversicherung. Erst der internen Revision fiel auf, dass der fröhliche Datentausch illegal war. Folksam entschuldigte sich. Ein Missbrauch der Daten sei bislang nicht bekannt, teilte die Firma mit (Illegaler Datenaustausch, SZ 05.11.2020, 20).

Spanien

Regierung erwägt Impfregister

Die Regierung Spaniens erwägt, Menschen, die sich nicht gegen Covid 19 impfen lassen wollen in einem Verzeichnis zu registrieren. Gesundheitsminister Salvador Illa sagte am 28.12.2020, Impfungen in Spanien würden sicher nicht verpflichtend werden. Doch wer eine Impfung angeboten bekomme und sich weigere, sie anzunehmen, könnte in einem Register gespeichert werden, das man mit europäischen Partnern teilen wolle. Diese Information solle aber nicht veröffentlicht, sondern „im höchsten Respekt vor dem Datenschutz“ verwendet werden. In Spanien ist die Zahl derer, die eine Impfung verweigern wollen, laut Umfragen von November auf Dezember 2020 von 47 auf 28% gesunken (Impfregister erwogen, SZ 30.12.2020, 7).

Türkei

Erdogan verlässt WhatsApp

Der türkische Präsident Recep Tayyip Erdogan verzichtet auf die weitere Nutzung des Messengers WhatsApp, nachdem der Dienst seine Datenschutzrichtlinie geändert hat. Er will künftig die aus der Türkei stammende App „BiP“, die zum Mobilfunkanbieter Turkcell gehört, nutzen. Künftig sollen auch Journalisten ihre Informationen ausschließlich über diesen Anbieter beziehen können. Zahlreiche Türken schlossen sich Erdogan nach der Veröffentlichung des neuen WhatsApp-Updates an, viele twitterten den Hashtag #DeletingWhatsapp.

Das WhatsApp-Update ist kontrovers und umstritten. Der Messenger-Dienst zwingt seine Nutzer dazu die neuen Datenschutzrichtlinien zu akzeptieren. In dem Update heißt es: „WhatsApp aktualisiert seine Nutzungsbedingungen und seine Datenschutzrichtlinie. Wesentliche Updates sind unter anderem mehr Informationen zu Folgendem: WhatsApp Service und wie wir deine Daten verarbeiten“. Darüber hinaus heißt es: „Wie Unternehmen mit von Facebook gehosteten Services ihre WhatsApp Chats speichern und verwalten können.“ Wer dem Update nicht zustimmte, konnte den Messenger-Dienst ab dem 08.02.2021 nicht mehr nutzen.

Das Update soll dazu dienen, dass WhatsApp und andere Facebook-Dienste Informationen miteinander austauschen können, um die Sicherheit und Integrität der Facebook-Produkte zu gewährleisten. Dazu heißt es: „Keine der Informationen, die WhatsApp auf dieser Grundlage weitergibt, dürfen für die eigenen Zwecke der Facebook-Unternehmen verwendet werden.“ Damit dürfen die Daten aus WhatsApp nicht zur Verbesserung des Anzeigesystems genutzt werden.

Ali Taha Koc, Chef des türkischen Presidental Digital Transformation Office unter Recep Tayyip Erdogan, kritisierte die neuen Datenschutzrichtlinien scharf. „Wir müssen unsere Daten mit lokaler und nationaler Software schützen und sie nach unseren Bedürfnissen entwickeln. Lassen Sie uns nicht vergessen, dass die Daten der Türkei in der Türkei dank lokaler und nationaler Lösungen bleiben werden“ (Ziegele, Nach kontroversem Datenschutz-Update: Erdogan verzichtet auf Whatsapp, www.fr.de 11.01.2021).

Israel

Vakzin gegen Daten

Während in der EU wegen Lieferengpässen der Zeitplan zum Impfstart gegen das Coronavirus stockt, hat Israel keine Lieferprobleme, obwohl das Land aus der EU versorgt wird. Nach BioNTech/Pfizer liefert auch AstraZeneca weniger Corona-Impfstoff an die EU-Staaten als nach Israel. Israel hatte von Anfang mehr Impfstoff zur Verfügung, als verimpft werden konnte.

Israel hat in den Impfstoff-Verhandlungen einen anderen Ansatz verfolgt als die EU und sich lange vor den Europäern große Impfstoff-Mengen von BioNTech/Pfizer gesichert. Vor allem hat das Land dem Impfstoffhersteller im Gegenzug die Übermittlung von Impfdaten vertraglich garantiert. Die EU legte hingegen großen Wert darauf, dass Pfizer die Produkthaftung übernimmt – was in Israel der Staat macht. Es spricht auch einiges dafür, dass Israel einen höheren Preis für die Dosen bezahlt als die EU. Israels Premier Benjamin Netanjahu rühmte sich, „17 Mal“ mit seinem „Freund“ Albert Bourla, CEO bei Pfizer, telefoniert zu haben. Das Ergebnis ist, so Israels Gesundheitsminister Juli Edelstein, eine „Win-win-Situation“.

Der Impfstoffhersteller verpflichtete sich Israel so lange mit Impfstoff zu ver-

sorgen, bis im Land eine Herdenimmunität, also eine Immunität von 95% der Bevölkerung, erreicht ist. Im Gegenzug versorgt das israelische Gesundheitsministerium Pfizer wöchentlich mit Informationen über die Impfungen. Dazu gehören Infektions- und Impfzahlen, aber auch die demografischen Angaben der Patienten wie zum Beispiel das Alter und Geschlecht. Die Daten werden laut israelischen Behörden anonymisiert an Pfizer geschickt.

Es gibt durchaus Kritik an dieser Vorgehensweise, etwa vom renommierten Israel Demokratie Institut (IDI), das beanstandet, dass dafür nicht die Zustimmung der Bürger eingeholt wurde. BioNTech erklärte, dass alle von den Erkenntnissen profitieren würden. Aus diesem Grunde hält auch das Robert Koch-Institut (RKI) enge Verbindungen mit Israel, so RKI-Präsident Lothar Wieler: „Während der gesamten Pandemie haben wir jederzeit unsere Ansichten ausgetauscht, damit wir voneinander lernen können. Wir müssen unsere Ideen mitteilen und uns darüber austauschen" (Sina/Lauck, Warum Israel genug Impfstoff hat, www.tagesschau.de 23.01.2021; Münch, Deal des Jahres, SZ 20.01.2021, 4).

USA

Datenpanne bei Oracle-Tochter

Die Oracle-Tochter Bluekai räumte im Juli 2020 eine Datenpanne ein: Da zwei Unternehmen die Data-Management-Plattform des Big-Data-Spezialisten nicht korrekt konfiguiert hatten, waren Milliarden Nutzerdaten im Netz frei verfügbar. Auch Deutsche waren von der Datensammlung per Cookies und anderen Tracking-Techniken betroffen. Die Daten wie Name, Wohnort, Mail-Adressen und Infos zu Surfverhalten, Einkäufen und Newslettern lassen Rückschlüsse sowohl auf Hobbys, als auch auf politische Einstellungen, Gesundheitszustand bis zu sexuellen Neigungen zu. Oracle wollte gegenüber der Presse weder die Namen der betroffenen Unternehmen mitteilen, noch, ob die Panne den Behörden gemeldet worden sei (Milliarden Nutzerdaten von Bluekai im Netz verfügbar, Computerwoche 28-29/2020 06.07.2020, 11).

USA

Digitaler Sicherheitsdienstler dringt in Intimbereich ein

T. A., ein 35-jähriger ehemaliger Angestellter des Heim- und Bürosicherheitsdienstes ADT, hat seine Position bei der US-amerikanischen Firma ausgenutzt, um mehr als fünf Jahre lang Kunden in intimen Situationen zu beobachten. Das gab er am 21.01.2021 vor einem Bezirksgericht im US-Bundesstaat Texas zu und bekannte sich unter anderem des Computerbetrugs (computer fraud) für schuldig. Ihm drohen nun bis zu fünf Jahre Haft. T.A. führte eine Liste von Kundenhaushalten mit attraktiven Frauen, deren Kundenkonten er seine E-Mail-Adresse hinzufügte. Damit hatte er Zugriff auf die Mobil-App des ADT-Dienstes Pulse, mit der Nutzer aus der Ferne Lichter an- oder ausschalten, Alarme de- oder reaktivieren oder das Bild der Kameras sehen können. Auf Kundennachfrage erklärte T.A., er benötige den Zugriff, um die Sicherheitsfunktionen zu testen. Stattdessen nutzte er die App über 9.600-mal, um die Frauen zu beobachten – vorzugsweise, wenn sie nackt waren, oder beim Sex.

Für T.A. könnte sich als besonders problematisch herausstellen, dass mindestens eine der Frauen zu dem Zeitpunkt minderjährig war. Allein auf die Kameras in ihrem Haus griff der Angeklagte beinahe 100-mal zu. Laut eigenen Angaben habe ADT das rechtswidrige Verhalten seines Mitarbeiters der Staatsanwaltschaft mitgeteilt, als die Firma davon Kenntnis erlangte, und kooperiere bei den Ermittlungen des FBI und der Staatsanwaltschaft. Dennoch strengen mehrere Parteien Sammelklagen gegen die Firma an. Eine davon vertritt die minderjährigen Familienmitglieder der Kunden. Kernanklagepunkt: ADT habe seinen Dienst als Möglichkeit beworben, Kinder und Haustiere aus der Ferne im Blick behalten zu können, es aber versäumt angemessene Sicherheitsvorkehrungen zu implementieren. Dazu hätten etwa Zwei-Faktor-Authentisierung oder SMS-Benachrichtigungen bei einer Neuanmeldung zählen müssen.

Bei solchen elektronischen Überwachungssystemen sollte sich der Kunde oder Nutzer grundsätzlich des Missbrauchspotenzials bewusst sein. Dabei ist es egal, ob er einen Dienstleister beauftragt oder die Ausstattung selbst in die Hand nimmt. Auch werden immer wieder Sicherheitslücken öffentlich, mit denen solche Systeme geknackt und belauscht oder anderweitig missbraucht werden (Kraft, Sicherheitsdienstleister: Angestellter bespitzelt über Kameras Kunden beim Sex, www.heise.de 23.01.2021, Kurzlink: https://heise.de/-5033734).

Brasilien

Vom Datenschutzpionier zum Datenschutzschlusslicht

Über viele Jahre hinweg nahm Brasilien als die größte Demokratie Lateinamerikas eine Vorreiterrolle beim Datenmanagement und beim Datenschutz ein. 1995 wurde der brasilianische Internet-Lenkungsausschuss ins Leben gerufen. Das Stakeholder-Gremium half, Grundsätze für die Internetverwaltung festzulegen. Angetrieben durch Edward Snowdens Enthüllungen, leistete die Regierung von Dilma Rousseff 2014 Pionierarbeit mit dem Marco Civil, einer Art „Internet Bill of Rights", die Tim Berners-Lee, der Erfinder des World Wide Web, lobte. Vier Jahre später verabschiedete der Kongress ein Datenschutzgesetz, das LGPD, das sich eng an die europäische Datenschutz-Grundverordnung anlehnt.

Die Zeiten änderten sich mit Präsident Jair Bolsonaro. Schon vor der Covid-19-Pandemie hatte Brasiliens Regierung begonnen eine umfassende Infrastruktur zur Datenerfassung und Überwachung aufzubauen. Im Oktober 2019 unterzeichnete Bolsonaro ein Dekret, das alle Bundesbehörden dazu verpflichtet einen Großteil der Informationen, die sie über brasilianische Staatsbürger besitzen – von Gesundheitsdaten bis hin zu biometrischen Angaben –, gemeinsam zu nutzen und in einer Master-Datenbank, dem Cadastro Base do Cidadão, abzulegen.

Durch den Informationsaustausch will die Regierung offiziell Qualität und Konsistenz ihrer Daten erhöhen, um öffentliche Dienstleistungen zu verbessern, Wahlbetrug einzudämmen und Bürokratie abzubauen. Kritiker warnen jedoch: Eine solche Datenkonzentration unter Bolsonaros rechtsextremer Führung könne leicht missbraucht werden, um Privatsphäre und bürgerliche Freiheiten einzuschränken. Der Spielraum bei der Datenerfassung ist groß. Neben Basisinformationen wie Name, Familienstand und Beschäftigung soll das Cadastro biometrische Informationen wie Gesichtsprofile, Stimmproben, Iris- und Netzhautscans, Abdrücke von Fingern und Handflächen und sogar ein Profil des Gangs aufnehmen. Dem Austausch von Gesundheitsdaten sind keine Grenzen gesetzt, selbst Gensequenzen dürfen weitergegeben werden (Kemeny, Brasiliens Weg in die Datendiktatur, www.heise.de 19.11.2020, Kurzlink: https://heise.de/-4964683).

Brasilien

Daten der gesamten Bevölkerung offenbar geleakt

Das brasilianische Labor für Cybersicherheit PSafe hat aufgedeckt, dass umfangreiche Datenbanken gehackt und so Datensätze von über 220 Mio. Brasilianern in Verbrecherhände gefallen sein dürften. Darin enthalten sind vollständige Namen, Geburtsdaten und Steuernummern (CPF). CPF spielen im brasilianischen Alltag eine bedeutende Rolle. Betroffen sind demnach auch Informationen über Unternehmen und Behörden. Die Einwohnerzahl Brasiliens ist mit 212 Millionen kleiner als die Zahl der erlangten Datensätze. Zusätzlich zu den personenbezogenen Daten seien noch Informationen über mehr als 104 Mio. Fahrzeuge dabei, einschließlich Fahrgestellnummer, Kennzeichen, Meldegemeinde, Farbe, Marke, Modell, Baujahr, Hubraum und Kraftstoffart. All diese Daten werden offenbar online zum Verkauf feilgeboten.

Wie die Daten erbeutet wurden, liegt im Dunkeln. Die Tageszeitung „Estadão" aus der Wirtschaftsmetropole São Paulo hält es für wahrscheinlich, dass es sich um eine Datenbank der Bonitätsbewertungsfirma Seresa Experian handelt. Sie ist das brasilianische Pendant zur deutschen Schufa und den nordamerikanischen Credit Bureaus Equifax, Transunion und Experian. Seresa Experian ist eine Tochterfirma Experians.

Seresa Experian bewertet die Kreditwürdigkeit von Verbrauchern und Unternehmern. Journalisten des Estadão berichten, sie hätten Zugang zu einem Teil der Daten bekommen; dort werde das Kreditbewertungsbüro erwähnt. Eine der Datenbanken gehört demnach zum Serasa-Dienst Mosaic. Das Unternehmen bestritt dies und versprach den Fall zu untersuchen.

Der Jurist und Datenschutzexperte Bruno Bioni von der gemeinnützigen Organisation Data Privacy Brasil erklärte: „Nach dem jetzigen Informationsstand handelt es sich um das größte und gefährlichste Datenleck in der Geschichte Brasiliens." Er vergleicht den Fall mit dem Hacker-Jackpot in den USA, als 2017 das Credit Bureau Equifax gehackt wurde und Daten über 145 Millionen Menschen erbeutet wurden (DANA 3/2017, 170 f.).

Emilio Simoni, Direktor des PSafe-Eigentümers dfndr lab, sieht erhebliches Gefahrenpotential für Verbraucher: „Diese Daten können leicht für Phishing verwendet werden. Sobald der Cyberkriminelle die CPF und andere tatsächliche Daten der Person hat, wäre es ein Leichtes, an kritischere Daten des Opfers zu gelangen, die zum Beispiel für die Beantragung von Krediten, Bankpasswörtern und die Beauftragung von Dienstleistungen verwendet werden könnten." Der Fall sei erst durch das Verkaufsangebot der Täter ans Tageslicht gekommen: „Die Cyberkriminellen stellen einen Teil der Datenbanken zur Verfügung, um den Wahrheitsgehalt der erlangten Informationen zu beweisen. Profit wollen sie machen, indem sie tiefer gehende Daten wie E-Mails, Telefone, Kaufkraftdaten und Berufe der betroffenen Personen verkaufen."

Das Datenleck dürfte die erste große Herausforderung der brasilianischen Datenschutzbehörde ANPD werden. Ein neues Datenschutzgesetz sieht empfindliche Strafen in Fällen wie diesem vor, tritt allerdings erst im August 2021 in Kraft (DANA 4/2018, 214 f.). Daher forderte Bioni die Verbraucherschutzzentrale Senacon auf sich sofort einzuschalten (Löding, 220 Millionen Datensätze geklaut: Gefahr für alle Steuerzahler Brasiliens, www.heise.de 26.01.2021; Kurzlink: https://heise.de/-5035563).

China

Social-Credit-System verzögert sich

Das 2014 offiziell angekündigte Sozialkreditsystem Chinas inklusive einer Bürgerbewertung in Form eines „Citizen Score" verspätet sich. Das Verfahren soll ein wesentlicher Teil des chinesischen Überwachungsnetzes und sollte laut dem Plan der Zentralregierung in Peking bis Ende 2020 landesweit etabliert sein. Daraus wurde aber nichts; bislang bleibt es bei einer Reihe verteilter Pilotprojekte in verschiedenen Städten und Regionen, die nicht interoperabel sind.

2014 stellte die kommunistische Staatsführung ihre Initiative für ein umfassendes soziales Kreditsystem auf Basis von Scoring-Verfahren der Finanzwirtschaft zur Bonitätsprüfung offiziell vor. Es soll demnach die soziale Integrität stärken, „gegenseitiges Vertrauen" fördern und soziale Konflikte verringern. Die chinesische Regierung erachtet das Vorhaben so als „dringende Voraussetzung für den Aufbau einer harmonischen sozialistischen Gesellschaft".

Qian Sun von der gemeinnützigen Organisation AlgorithmWatch beschreibt, dass die Vorgeschichte des Großprojekts bis 1999 zurückreicht. Einer der wichtigsten Köpfe hinter dem System, Lin Junyue, soll das System demnach vor über 20 Jahren gefordert und geplant haben, um gegen Betrug und Fälschungen auf dem chinesischen Markt vorzugehen. Damals sei es im Wesentlichen auf den Finanzbereich ausgerichtet gewesen, um die Kreditfähigkeit von Käufern zu beurteilen und den Bruch vertraglicher Pflichten zu ahnden.

2012 erweiterte Chinas mächtige Nationale Entwicklungs- und Reformkommission das Konzept um ein automatisiertes Bewertungsverfahren für soziale Integrität. Blaupausen für den „Citizen

Score“ im Bereich Finanzen lieferten parallel der E-Commerce-Riese Alibaba über seine Tochter Ant Financial Services mit „Sesame Credit“ sowie Tencent mit dem App-System WeChat. Die Zentralbank verweigerte 2018 aber neun einschlägigen Auskunfteien inklusive der von Jack Ma geführten Ant Financial die Lizenz für die Teilnahme am geplanten nationalen sozialen Kreditsystem.

Zuvor hatten die Zentralbank und die Reformkommission 2015 und 2016 insgesamt 43 Pilotprojekte in Regionen und Städten ins Auge gefasst. Für konkrete Tests wählten sie letztlich 28 aus, zu denen Metropolen wie Schanghai und Suzhou gehören. Mit Punktabzügen und Strafen wie Sperren für Schnellzüge, Flüge, Luxushotels oder schnelles Internet muss dort etwa rechnen, wer zu viel Zeit mit Computerspielen verbringt, bei Rot über die Ampel geht, vor Fußgängerüberwegen nicht hält oder ein bestelltes Taxi nicht nimmt. Gerichte sollen mit diesem Instrument bis Mitte 2019 allein 27 Millionen Bürger auf die „No Fly“-Liste gesetzt haben. 14 Millionen wurde die Bonität abgesprochen. Zu den Gesundheitsdaten, die die Systeme einschließen, gehören seit 2020 auch Ergebnisse von Tests auf das neuartige Coronavirus.

Eine repräsentative Umfrage des Instituts für Chinastudien der FU Berlin von 2018 hatte ergeben, dass 80% der chinesischen Online-Nutzer das Vorhaben befürworteten. Viele Menschen empfanden ein solches System demnach etwa als wichtig, um „institutionelle und regulatorische Lücken zu schließen“. Doch die Einstellung dazu scheint sich gewandelt zu haben. Laut der staatlichen Nachrichtenagentur Xinhua sorgten sich bei einer Umfrage im Juli 2020 70% der Teilnehmer über möglichen Missbrauch des Bewertungsverfahrens.

Der Wettbewerb zwischen verschiedenen staatlichen Kommissionen und lokalen Behörden hat gemäß AlgorithmWatch dazu geführt die Definition von „Kredit“ zu überdehnen, was die zunehmende Skepsis in der Bevölkerung erklärt. Ende 2019 habe die Nationale Gesundheitskommission etwa darum gebeten Blutspenden einzubeziehen. Obwohl Städte wie Suzhou solche Aktivitäten bereits berücksichtigt hätten, „löste der Schritt heftige Diskussionen innerhalb Chinas aus“. Wang Lu etwa, ein Ex-Manager der Zentralbank, habe gewarnt, dass fast alle sozialen Probleme in den „Korb“ des Sozialkredits geworfen würden.

Kritiker beschreiben das System auch als zu chaotisch. Es gebe keine zentrale Koordination und kein grundlegendes rechtliches Rahmenwerk. Dezember 2020 veröffentlichte die Regierung zwar Richtlinien für Korrekturen; Lokale Behörden hätten die Definition von „schlechtem Verhalten“ falsch verstanden. Spucken in der Öffentlichkeit und Schwarzfahren etwa sollten nicht in die Bewertung einfließen. Das angekündigte nationale Gesetz für den Ausbau und die Vereinheitlichung des Systems lässt weiter auf sich warten. Nach Ansicht von Jeremy Daum, Forscher am Paul Tsai China Center an der Yale Law School, geht es der Regierung in Peking im Kern um Propaganda. Den Bürgern solle beigebracht werden ehrlich zu sein. Die Rede vom „Citizen Score“ habe vor allem erzieherischen Charakter (Krempl, Citizen Score: Chinas soziales Kreditsystem nicht mehr im Plan, www.heise.de 19.01.2021, Kurzlink: https://heise.de/-5028166).

Technik-Nachrichten

Microsoft-Patent kontrolliert Körpersprache und Gesichtsmimik

Microsoft hat ein Patent für ein System beantragt, das die Körpersprache und Gesichtsausdrücke von Mitarbeitern in einer Konferenz überwacht. Dies soll der Effektivitätssteigerung und Sicherheit der Mitarbeiter dienen. In dem dafür eingereichten US-Patentantrag ist von „Qualitätssicherung“ die Rede. Sensoren überwachen mit dem „Meeting Inside Computing System“ die Körpersprache und Gesichtsausdrücke der anwesenden Personen in einem Raum oder bei einem Online-Meeting. Dafür wird der Konferenzraum mit Kameras ausgestattet. Die Daten werden ausgewertet und mit vorangegangenen Meetings abgeglichen. Das System macht dann entsprechende Verbesserungsvorschläge für kommende Konferenzen. Das kann ein Raumwechseln sein oder die Zeit, zu der die Mitarbeiter am fittesten erscheinen.

Bei Microsoft heißt es in dem Antrag, dass viele Systeme existieren, die der Buchung von Räumen dienen, dabei aber außer Acht lassen, dass jemand beispielsweise sieben Mitarbeiter für eine Konferenz in einen Raum einlädt, der nur für vier Menschen angenehm ist. Oder dass ein Mitarbeiter einen Raum für den Nachmittag bucht, obwohl dieser gerade dann besonders warm und dadurch unangenehm ist: „Bisherigen Buchungsplattformen fehlt der Kontext zur realen Welt.“ Das könne nicht nur dazu führen, dass Meetings unproduktiv werden, sondern sogar negative Auswirkungen auf die Gesundheit der Mitarbeiter haben. Also sei es nötig, Qualitätsparameter festzulegen und einfließen zu lassen.

Potenziell ließen sich auch die Smartphones der Mitarbeiter mit dem System verknüpfen, um zu sehen, ob jemand nebenher etwas anderes macht. Zudem könne die Sprache daraufhin ausgewertet werden, ob jemand müde ist oder gelangweilt, so Microsoft. Ein Microsoft-Sprecher erklärte, dass man viele Patente einreiche, diese aber nicht unbedingt auch tatsächlich umgesetzt werden würden.

Anwenderüberwachung ist bei Microsoft kein ganz neues Thema. Auch die Office-Suite 365 kann um Funktionen erweitert werden, mit denen Unternehmen die Arbeitsgepflogenheiten ihrer Belegschaft detailliert beobachten können. Das nennt sich dann „Workplace Analytics" und berechnet einen „Productivity Score". Neben Technik-Informationen, die etwa aufzeigen, wie viel Zeit verloren geht, wenn Mitarbeiter-PCs mit konventionellen Festplatten booten statt mit SSDs, sammelt die Software auch Informationen darüber, an wie vielen Tagen ein Mitarbeiter E-Mails und Yammer-Nachrichten verschickt, sowie welche Chat- und Nachrichtenkanäle er genutzt hat (Weiß, Microsoft beantragt Patent für Gesichts- und Körpersprache-Sensoren, www.heise.de 01.12.2020, Kurzlink: https://heise.de/-4976505).

Rechtsprechung

OGH Österreich

Weltweite Löschpflicht Facebooks bestätigt

Der Oberste Gerichtshof (OGH) Österreichs hat mit Urteil vom 12.11.2020 das soziale Netzwerk Facebook verpflichtet, Beleidigungen der Grünen-Politikerin Eva Glawischnig-Piesczek und sinngleiche Einträge weltweit zu löschen (Az. 6 Ob 195/19y). Damit bestätigen die Richter in Wien in dem schon Jahre dauernden Rechtsstreit die vorinstanzliche Entscheidung. 2019 hatte auch der Europäische Gerichtshof (EuGH) geurteilt, dass Facebook gezwungen werden kann, Beleidigungen nicht nur im jeweils betroffenen Land, sondern für alle Nutzer zu löschen (DANA 4/2019, 235 f.). Mark Zuckerberg hatte das als bedenklich bezeichnet.

In dem Rechtsstreit geht es um Einträge auf Facebook, in denen ein Nutzer die damalige Vorsitzende der Grünen Österreichs als „korrupter Trampel" und „miese Volksverräterin" bezeichnet hatte. Nach einer Unterlassungsverfügung hatte die Politikerin auch die Löschung wortgleicher und sinngleicher Beiträge gefordert. Der später angerufene EuGH hatte entschieden, dass Facebook tatsächlich gezwungen werden kann, ähnliche und gleichlautende Ehrbeleidigungen und Diffamierungen zu suchen beziehungsweise weltweit zu löschen. Facebook war dem nicht nachgekommen und hatte den Eintrag nur in Österreich entfernt.

Der OGH schloss sich dem nun an und gab Glawischnig-Piesczek in ihrer Forderung Recht: Facebook müsse weltweit verhindern, dass Inhalte verbreitet und veröffentlicht werden, in denen die genannten Beleidigungen beziehungsweise sinngleiche vorkommen. Das gelte auch für die Äußerung, die Politikerin sei Mitglied einer „Faschistenpartei". Bei dem Urteil handelt es sich um die Letztentscheidung in dem sogenannten Sicherungsverfahren. Zwar steht noch das Hauptverfahren aus. In diesem gehe es aber nicht mehr um den Umgang mit den Beiträgen, sondern um die Herausgabe der Nutzerdaten, um Schadensersatzansprüche und die Frage der Urteilsveröffentlichung (Holland, Oberster Gerichtshof Österreichs: Facebook muss Beleidigungen weltweit löschen, www.heise.de 12.11.2020, Kurzlink: https://heise.de/-4958768).

Britischer High Court

Staatliche Hackingziele sind präzise zu benennen

Der britische High Court, der bedeutende Fälle in erster Instanz behandelt, hat in einem Urteil vom 09.01.2021 die bisherige breite Befugnis der Spionagebehörde GCHQ für internationale Cyberangriffe eingegrenzt. Der Geheimdienst darf demnach nicht mehr im Ausland auf Basis allgemeiner, nicht auf spezifische Maßnahmen ausgerichteter Gerichtsanordnungen – etwa per Staatstrojaner – in Smartphones, Computer und ganze Netzwerke eindringen.

Die Richter stellten auf Klage der Bürgerrechtsorganisation Privacy International hin fest, dass Abschnitt 5 des Intelligence Services Act (ISA) von 1994 es Sicherheitsbehörden wie Geheimdiensten nicht erlaubt sich auf solche breiten „thematischen" Durchsuchungsbefehle zum Hacken von IT-Systemen und Kommunikationsnetzen zu stützen. Konkrete Ziele der Spionage müssten in entsprechenden Anordnungen klar benannt werden. Nur so könnten die grundlegenden Verfassungsprinzipien des Vereinigten Königreichs und die Bestimmungen des allgemeinen britischen Rechts eingehalten werden.

In dem Urteil untermauert der High Court das Prinzip, dass ein Durchsuchungsbefehl nicht so weit gefasst sein darf, dass er den Ausführenden einen erheblichen Ermessensspielraum einräumt. Er kann sich etwa nicht auf eine ganze Klasse von Gegenständen, Personen oder Verhaltensweisen erstrecken wie etwa „alle Mobiltelefone, die von einem Mitglied einer kriminellen Vereinigung benutzt werden". Vielmehr müssen etwa die Namen, Standorte oder Kennungen Verdächtigter angegeben werden.

Laut dem britischen Überwachungsgesetz „Investigatory Powers Act" von 2016 darf der GCHQ massive Eingriffe in technische Gerätschaften vornehmen. Die britische Regierung hatte 2018 die Parole ausgegeben, dass der Geheimdienst diese zunächst für Einzelfälle in Ausnahmen vorgesehene Kompetenz öfter anwenden solle und damit erneut Proteste bei Datenschützern ausgelöst.

Privacy International geht seit vielen Jahren gegen diese Ermächtigung zur Massenüberwachung vor. Die Beschwerdeführer hatten sich 2014 zunächst an

das zuständige nationale Gericht gewandt, das Investigatory Powers Tribunal (IPT). Dieses hatte die Klage 2016 zurückgewiesen, aber erstmals die massiven, von Edward Snowden publik gemachten GCHQ-Spionageaktivitäten bestätigt und „ernsthafte Fragen“ damit verknüpft.

Die Aktivisten verfolgten ihr Anliegen weiter durch die Instanzen. 2019 gab ihnen schließlich der Supreme Court weitgehend Recht. Das oberste britische Gericht urteilte, dass Entscheidungen des IPT vom High Court überprüft werden können und das Prinzip der Rechtsstaatlichkeit gewährt werden muss. Privacy International wandte sich daraufhin erneut an die zuständige Instanz und erstritt nun die Klarstellungen. Der IPT beziehungsweise die britische Regierung können dagegen noch in Berufung gehen. Tun sie dies nicht, müssen sie die Anordnungspraxis einschränken.

2018 hatte der Supreme Court schon entschieden, dass die britischen Geheimdienste GCHQ, MI5 und MI6 sich jahrelang illegal massenhaft Zugang zu Daten von Internetnutzern verschafft hatten. Caroline Wilson Palow, Justiziarin von Privacy International, sprach angesichts der Ansage des High Court nun von einem historischen Sieg. Dieser übertrage 250 Jahre alte Rechtsprinzipien in die Neuzeit. Die Regierung sei viel zu lang mit den viel zu breiten Anordnungen durchgekommen (Krempl, Spionage: Britisches Gericht schränkt massenhaftes GCHQ-Hacking ein, www.heise.de 10.01.2021, Kurzlink: https://heise.de/-5019452).

BVerfG

Antiterrordatei-Regelung zu Data-Mining verfassungswidrig

Das Bundesverfassungsgericht (BVerfG) hat mit Beschluss vom 11.12.2020 die Regelungen zur Antiterrordatei (ATD) in Teilen für verfassungswidrig erklärt (Az. 1 BvR 3214/15). Es entsprach damit dem Beschwerdeführer, der sich durch § 6a Abs. 2 Satz 1 des der Datei zugrundeliegenden Gesetzes (ATDG) in seinem Grundrecht auf informationelle Selbstbestimmung verletzt sieht. § 6a ATDG ermächtigt die Sicherheitsbehörden erstmalig zur erweiterten Nutzung, also Data Mining von Datenarten, die in der Antiterrordatei gespeichert sind. Das gelte über den Datenaustausch unter den Behörden hinaus auch zur operativen Aufgabenwahrnehmung: „§ 6a ATDG gestattet damit die unmittelbare Nutzung der Antiterrordatei auch zur Generierung neuer Erkenntnisse aus den Querverbindungen der gespeicherten Datensätze. Dies war bisher nur in Eilfällen möglich.“

Das BVerfG stellte fest, dass der beanstandete § 6a Abs. 2 Satz 1 nicht dem informationellen Trennungsprinzip entspricht. Wenn Polizeibehörden eine Verbunddatei erweitert nutzten und es dadurch zu mehr Belastungen komme, müsse dies „auf der Grundlage präzise bestimmter und normenklarer Regelungen an hinreichende Eingriffsschwellen gebunden sein“. Dem genügt § 6a ATDG nicht.

Die 2006 beschlossene und 2007 eingerichtete Antiterrordatei (ATD) wird vom Bundeskriminalamt (BKA) geführt und steht den Polizeibehörden und Nachrichtendiensten des Bundes und der Länder zur Verfügung. Die Datensammlung soll helfen, durch schnellen Informationsaustausch insbesondere islamistische Terroranschläge zu verhindern. Die ATD war zunächst als Verbunddatei für 38 Ämter und Geheimdienste lediglich als Fundstellennachweis ausgestaltet. Ein direkter Zugriff war nur auf wenige Grunddaten von Personen aus der Terrorszene erlaubt, etwa Name, Anschrift, Staatsangehörigkeit. Wer Details erfahren wollte – etwa die Tätigkeit in Infrastrukturbetrieben oder terrorismusrelevante Fähigkeiten – musste sich die Freigabe der speichernden Behörde holen.

Mit Urteil vom 24.04.2013 hatte das BVerfG mehrere Vorschriften des Gesetzes für unvereinbar mit dem Grundgesetz erklärt (Az. 1 BvR 1215/07). Der Kreis der damals 18.000 gespeicherten Personen war dem Gericht zu opulent. Kontaktpersonen durften nicht mehr so einfach gespeichert werden. Menschen sollten nicht ohne eigenes Zutun in die Mühlen der Sicherheitsbehörden geraten können. Schon damals mahnte das Gericht nachdrücklich eine „informationelle“ Trennung zwischen Polizei und Geheimdiensten an. Der Grundgedanke dabei ist, dass die Nachrichtendienste freier bei der Informationserhebung sind, weil sie im Unterschied zur Polizei keine operativen Befugnisse haben. Diese Unterschiede dürfen nicht durch die Hintertür des Informationsaustauschs verwischt werden. Daraufhin änderte der Gesetzgeber die beanstandeten Vorschriften und ergänzte das ATDG 2015 um den Paragraph 6a, der eine „erweiterte Nutzung“ der Daten erlaubt und um den es nun in Karlsruhe ging. Seinerzeit klagte wie diesmal ein pensionierter Richter.

Die angegriffene Vorschrift hat folgenden Wortlaut: „Eine beteiligte Behörde des Bundes darf zur Erfüllung ihrer gesetzlichen Aufgaben die in der Datei nach § 3 gespeicherten Datenarten mit Ausnahme der nach § 4 verdeckt gespeicherten Daten erweitert nutzen, soweit dies im Rahmen eines bestimmten einzelfallbezogenen Projekts für die Verfolgung qualifizierter Straftaten des internationalen Terrorismus im Einzelfall erforderlich ist, um weitere Zusammenhänge des Einzelfalls aufzuklären.“

Das Bundesamt für Verfassungsschutz (BfV) hatte für die erweiterte Nutzung mit dem damit verbundenen „erheblichen Mehrwert“ geworben. Mit der Datenanalyse könnten z.B. Reisewege nach Syrien oder in den Irak mit sonstigen Verdachtsmomenten verknüpft werden und so neue Ermittlungsansätze generiert werden. Ein solches „Data Mining“ war gemäß BfV-Angaben bisher noch nicht im Einsatz. Das BVerfG meint, dass für die erweiterte Nutzung der ATD zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr vorliegen müssen. Auch müsse die erweiterte Nutzung zur Informationsauswertung zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten sein. Zur Verfolgung einer Straftat bedürfe es eines begründeten Verdachts, für den konkrete und verdichtete Umstände als Tatsachenbasis vorhanden sind (Wilkens, Antiterrordatei-Gesetz ist teilweise verfassungswidrig, www.heise.de 11.12.2020; Kurzlink: https://heise.de/-4986674; Janisch, Nur bei konkreter Gefahr, SZ 12./13.12.2020, 8).

BVerwG

Rolf Gössner nach 40 Jahren BfV-Beobachtung höchstrichterlich rehabilitiert

Das Bundesverwaltungsgericht (BVerwG) hat mit Urteil vom 14.12.2020 in dritter und letzter Instanz nach 15 Jahren Verfahrensdauer ein Urteil des Oberverwaltungsgerichts NRW aus dem Jahr 2018 in vollem Umfang bestätigt, wonach die 38 Jahre währende geheimdienstliche Überwachung und Ausforschung des Rechtsanwalts, Publizisten und Bürgerrechtlers Rolf Gössner durch das beklagte Bundesamt für Verfassungsschutz (BfV) unverhältnismäßig und grundrechtswidrig war (Az. 6 C 11.18).

Das BfV hatte Rolf Gössner zum „Staats- und Verfassungsfeind" erklärt. Mit dem Urteil des BVerwG ist er nun endgültig rechtskräftig rehabilitiert. Das Verfahren endete gegen ein BfV, das zuletzt von Bundesinnenminister Horst Seehofer (CSU) und zuvor seit 1970 von weiteren 13 Bundesinnenministern und 12 BfV-Präsidenten verantwortet wurde.

Rolf Gössner sieht in den Urteilen des BVerwG und der vorangegangenen Instanzen einen „gerichtlichen Sieg über geheimdienstliche Verleumdungen und Willkür sowie über antidemokratische Denk-, Interpretations- und Handlungsmuster eines staatlichen Sicherheitsorgans" und „eine klare Entscheidung zugunsten der Meinungs-, Presse- und Berufsfreiheit und der informationellen Selbstbestimmung".

Der Prozessvertreter von Gössner Rechtsanwalt Udo Kauß wies darauf hin, dass sich der „Verfassungsschutz" 15 Jahre lang erbittert gegen die Verdikte der Justiz zur Wehr gesetzt hat. Gesinnungsschnüffelei und Gesinnungskontrolle müssten rechtssicher unterbunden werden, „nicht nur zum Schutze von – u.a. anwaltlichen – Berufsgeheimnissen, die unter Überwachungsbedingungen nicht mehr zu gewährleisten sind, sondern gegenüber Jedermann."

Gössner war seit 1970 vier Jahrzehnte lang ununterbrochen vom BfV geheimdienstlich beobachtet und ausgeforscht worden – schon als Jurastudent, später als Gerichtsreferendar und seitdem ein Arbeitsleben lang in allen seinen beruflichen und ehrenamtlichen Funktionen als Publizist, Rechtsanwalt, parlamentarischer Berater, später auch als Präsident der Internationalen Liga für Menschenrechte und seit 2007 zudem als stellvertretender Richter am Staatsgerichtshof der Freien Hansestadt Bremen. Es dürfte die längste Dauerbeobachtung einer unabhängigen, parteilosen Einzelperson durch den Inlandsgeheimdienst sein, die bislang dokumentiert werden konnte.

Zur Last gelegt wurden ihm berufliche und ehrenamtliche Kontakte zu angeblich „linksextremistischen" und „linksextremistisch beeinflussten" Gruppen und Veranstaltern, bei denen er referierte und diskutierte, aber auch zu bestimmten Presseorganen, in denen er – neben vielen anderen Medien – veröffentlichte, denen er Interviews gab oder in denen über seine Aktivitäten berichtet wurde. Mit seinen Kontakten, publizistischen Beiträgen und Vorträgen soll er, so die Unterstellung, nicht verbotene, aber vom BfV als „linksextremistisch" eingestufte Gruppen und Organe „nachdrücklich unterstützt" haben; er soll sie – so wörtlich – als „prominenter Jurist" aufgewertet und gesellschaftsfähig gemacht haben. Aus vollkommen legalen und legitimen Berufskontakten wurde so eine Art von Kontaktschuld konstruiert.

Im Laufe des 15-jährigen Klageverfahrens hatte das BfV dann neue Vorwürfe gegen Gössner nachgeschoben, die zuvor keinerlei Rolle gespielt hatten. Auf Misskredit stieß insbesondere Gössners inhaltlich begründete Kritik an der bundesdeutschen Sicherheits- und Antiterrorpolitik und an den Sicherheitsorganen.

Über den Einzelfall hinausgehend hat das Urteil des BVerwG Bedeutung für andere Publizisten, Anwälte und Menschenrechtler in Bezug auf das Mandatsgeheimnis und den Informantenschutz. Die verfassungsrechtlich geschützten Vertrauensverhältnisse zwischen Anwalt und Mandant sowie zwischen Journalist und Informant, die Berufsfreiheit und berufliche Praxis waren durch die Beobachtung und Diskreditierung Gössners beeinträchtigt (PE RA Kauß, Vier Jahrzehnte „Verfassungsschutz"-Skandal rechtskräftig beendet, 17.12.2020).

BGH

Bei Urheberrechtsverstoß gibt es nur die Postadresse

Der Bundesgerichtshof (BGH) hat mit Urteil vom 10.12.2020 auf eine Klage des Filmverleihers Constantin gegen Youtube entschieden, dass die Videoplattform bei einer Urheberrechtsverletzung nicht mehr als die Postanschrift an den Kläger herausrücken muss (Az. I ZR 153/17). Dieser wollte der Filmindustrie wirksamere Instrumente im Kampf gegen illegale Uploads verschaffen und eine Auskunft auch über Mail- und IP-Adressen der Nutzer durchsetzen.

Mit der Postanschrift können aber Unternehmen wie die Constantin wenig anfangen: Wer illegal Filme hochlädt, gibt selten seine korrekte Anschrift an, sondern eher – wie im verhandelten Fall – einen falschen Namen und eine Fantasieadresse. Die Anwälte von Constantin-Film pochten deshalb darauf, dass die einschlägigen Vorschriften ihnen doch auch Zugriff auf weitere Daten gewähren müssten, mit denen sie die Verdächtigen aufspüren können. Im deutschen Urhebergesetz bezieht sich der Auskunftsanspruch allerdings nur auf „Name und Anschrift", in der einschlägigen EU-Richtlinie ist von „Namen und Adressen" die Rede. Der BGH hatte den Europäischen Gerichtshof (EuGH) zur Klärung der Frage angerufen. Das EuGH-Urteil vom 09.07.2020 gab das vor, was der BGH nun nachgezeichnet hat (C-264/17): Es besteht kein Anspruch auf Mail- oder IP-Adressen oder Telefonnummern, sondern lediglich darauf, dass Youtube die altmodische Postadresse übermittelt. Womit die Auskunftsklagen weitgehend ins Leere gehen. Der Senatsvorsitzende Thomas Koch erklärte bei der Urteilsverkündung: „Die Entscheidung des EuGH ist für uns bindend."

Unternehmen greifen in der Praxis inzwischen auf andere Instrumente zurück, um gegen illegale Uploads vorzugehen. Google hat für Youtube ein Content-ID-System entwickelt, eine Art Datenbank, in der die Medienkonzerne ihre Dateien für den Abgleich auf Youtube abspeichern. Hochgeladene Filme können dann entweder geblockt oder zu Geld gemacht werden, indem der Rechteinhaber Werbung schaltet.

Viele Medienkonzerne haben ohnehin Lizenzvereinbarungen mit Youtube geschlossen, wie ein Youtube-Anwalt am Rande der Verhandlung Oktober 2020 erläutert hatte. Über so eine Lizenz profitieren die Produzenten sogar finanziell von den Uploads, und Youtube bleibt als Plattform attraktiv.

Derweil wird der Schutz der Urheber neu aufgestellt. Das Bundesjustizministerium legte einen Referentenentwurf vor, mit dem mehrere EU-Urheberrechts-Richtlinien in deutsches Recht umgesetzt werden sollen. Teil der Reform ist auch eine wirksamere Haftung von Plattformen wie Youtube. Entweder müssen diese demnach Lizenzen für die hochgeladenen Filme und Lieder kaufen oder dafür sorgen, dass sie von ihrer Plattform verschwinden (Janisch, Adresse genügt, SZ 11.12.2020, 21).

BSG

Kein Anspruch auf analoge Krankenversichertenkarte

Gesetzlich Krankenversicherte können gemäß einem Urteil des Bundessozialgerichts (BSG) vom 20.01.2021 von ihrer Krankenkasse keinen Nachweis ihrer Versicherung auf Papier als Alternative zur elektronischen Gesundheitskarte (eGK) verlangen. Die Kasseler Richter haben in zwei Verfahren aus Nordrhein-Westfalen und Rheinland-Pfalz entschieden (Az. B 1 KR 7/20 R sowie B 1 KR 15/20 R). Sie stellten fest, dass die gesetzlichen Regelungen zur eGK im Einklang mit der Europäischen Datenschutz-Grundverordnung (DS-GVO) stehen und die Kläger auch nicht in ihren Grundrechten verletzen.

Um Leistungen der Krankenversicherung in Anspruch nehmen zu können, müssen Versicherte ihre Berechtigung mit der Gesundheitskarte nachweisen. Auf dem Chip sind Versichertendaten wie Name, Anschrift, Versichertenstatus und -nummer gespeichert. Die beiden Kläger hatten unter anderem Datenschutzbedenken vorgebracht und sahen sich in ihrem Recht auf informationelle Selbstbestimmung verletzt. Die auf der Chipkarte gespeicherten Daten und die dahinter stehende zentralisierte Datenverarbeitung seien nicht sicher (Kein Anspruch auf papierenen Ersatz für elektronische Gesundheitskarte, www.heise.de 21.01.2021, Kurzlink: https://heise.de/-5031259).

OLG München

Facebooks Klarnamenpflicht ist zulässig

Das Oberlandesgericht (OLG) München entschied am 08.12.2020 in zwei Fällen zugunsten des sozialen Netzwerks Facebook, dass dieses Nutzer die Verwendung von Pseudonymen verbieten kann und befand damit dessen sogenannte Klarnamenpflicht für rechtens (Az. 18 U 2822/19 Pre und 18 U 5493/19 Pre). Facebook habe „angesichts eines mittlerweile weit verbreiteten sozialschädlichen Verhaltens im Internet" ein berechtigtes Interesse, so bereits präventiv auf seine Nutzer einzuwirken.

In den beiden vorliegenden Fällen hatte Facebook die Profile zweier Personen gesperrt, die Fantasienamen verwendeten. Die Landgerichte Traunstein und Ingolstadt hatten dazu in erster Instanz unterschiedlich entschieden. In Ingolstadt war die Klarnamenpflicht verworfen, in Traunstein bestätigt worden. Beim in Traunstein verhandelten Fall waren zudem rassistische Postings über schwarze Kannibalen und einen tanzenden Adolf Hitler hinzugekommen.

Das OLG München entschied, dass Facebook nicht gemäß § 13 Abs. 6 S. 1 Telemediengesetz (TMG) verpflichtet sei die Nutzung der Dienste unter einem Pseudonym zu ermöglichen. Die AGB von Facebook, die den Nutzer verpflichten den im bürgerlichen Alltag verwendeten Namen anzugeben, sei rechtens. Das TMG ist gemäß der Entscheidung grundsätzlich anwendbar. Zwar hat Facebook seinen Sitz in Irland. Für Verbraucher mit ständigem Wohnsitz in Deutschland gelte jedoch gemäß den Nutzungsbedingungen deutsches Recht. § 13 Abs. 6 S. 1 TMG werde auch nicht durch die Datenschutz-Grundverordnung (DSGVO) verdrängt. Zwar enthalte die DSGVO, die grundsätzlich vorrangig anwendbar sei, keine dem § 13 Abs. 6 S. 1 TMG entsprechende Bestimmung. Die Entstehungsgeschichte der DSGVO zeige zudem, dass dies vom Gesetzgeber so gewollt war. Er habe bewusst davon abgesehen, Anbieter von Telemedien zu verpflichten, die anonyme oder pseudonyme Nutzung zu gestatten.

Diese Entstehungsgeschichte lässt das OLG in die Zumutbarkeitsprüfung nach § 13 Abs. 6 S. 1 TMG einfließen und löst den Konflikt über eine europarechtskonforme Auslegung. Die Vorschrift verpflichte den Anbieter von Telemedien nämlich nur insoweit dazu, eine anonyme oder pseudonyme Nutzung zu ermöglichen, als ihm das zumutbar ist. Aufgrund der Entstehungsgeschichte der DSGVO sei Facebook hierbei ein großer Spielraum zuzusichern.

Diesen Spielraum habe Facebook nicht überschritten. Facebook begründet die in seinen Nutzungsbedingungen festgelegte Klarnamenpflicht folgendermaßen: „Wenn Personen hinter ihren Meinungen und Handlungen stehen, ist unsere Gemeinschaft sicherer und kann stärker zur Rechenschaft gezogen werden." Dieser Begründung folgt das OLG. Die Verpflichtung zur Verwendung des echten Namens sei geeignet, Nutzer von einem rechtswidrigen Verhalten im Internet abzuhalten: „Bei der Verwendung eines Pseudonyms liegt die Hemmschwelle nach allgemeiner Lebenserfahrung deutlich niedriger." Facebook sei daher nicht zumutbar, die Verwendung von Pseudonymen zu ermöglichen (Facebook darf Pseudonyme verbieten, www.lto.de 08.12.2020).

OLG Dresden

Sofortige E-Mail-Account-Löschung nach Vertragsbeendigung ist unzulässig

Gemäß einem Beschluss des Oberlandesgerichts Dresden (OLG) vom 05.09.2012 darf nach Beendigung eines Vertragsverhältnis der betriebliche E-Mail-Account erst gelöscht werden, wenn der ehemalige Inhaber an der Nutzung des Accounts kein Interesse mehr hat (4 W 961/12). Einem Fahrradkurier wurde während seiner Tätigkeit für einen Kurierdienst ein E-Mail-Account zur Verfügung gestellt. Nachdem das Vertragsverhältnis beendet wurde, löschte das Unternehmen den Account. Der Kurier verlangte Herausgabe der

unter seinem ehemaligen Account abgespeicherten E-Mails. Da das Landgericht Leipzig einen Herausgabeanspruch verneinte, wendete er sich an das Oberlandesgericht Dresden.

Das OLG verneinte einen Anspruch auf Herausgabe der Daten an den Kurier, da der Kurierdienst aufgrund der Löschung des Accounts keinen Zugriff mehr auf die Daten hatte. Die Herausgabe sei ihm daher nicht mehr möglich gewesen (§ 275 Abs. 1 BGB). Es bestätigte aber einen Anspruch auf Schadenersatz wegen eines Verstoßes gegen vertragliche Nebenpflichten (§ 280 BGB). Werde nämlich im Zusammenhang eines Vertragsverhältnisses dem Beschäftigten ein E-Mail-Account zur Verfügung gestellt, auf dem dieser auch private E-Mails abspeichern darf, entspreche es den vertraglichen Nebenpflichten, den Account nach Beendigung der Zusammenarbeit solange nicht zu löschen, bis klar sei, dass der Beschäftigte kein Interesse mehr an der Nutzung des Accounts hat. Zudem begründete das OLG den Schadensersatzanspruch mit § 823 Abs. 2 BGB in Verbindung mit § 303a StGB, da die Löschung des Accounts eine strafbare Löschung und Unbrauchbarmachung von Daten gemäß § 303a StGB dargestellt habe (Betrieblicher E-Mail-Account darf nicht sofort nach Beendigung des Vertragsverhältnisses gelöscht werden, www.kostenlose-urteile.de).

LG Bonn

BfDI-Strafe gegen 1&1 reduziert

Das Landgericht Bonn (LG) hat mit Urteil vom 11.11.2020 eine 9,6-Millionen-Euro-Strafe des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) Ulrich Kelber wegen DSGVO-Verstoßes gegen die 1&1 Telecom GmbH für unverhältnismäßig erklärt und reduziert. 1&1 soll jetzt 900.000 Euro zahlen. Das Verschulden des Unternehmens aus Montabaur in Rheinland-Pfalz bei der Herausgabe von Kundendaten ist nach Ansicht des Gerichts gering.

Bei dem Datenschutzverstoß ging es um den Anruf einer Frau bei der 1&1-Hotline im Jahr 2018. Die Stalkerin bekam die neue Handynummer ihres Ex-Mannes heraus, nur indem sie seinen Namen und sein Geburtsdatum nannte – das hätte nicht geschehen dürfen. In diesem laxen Authentifizierungsverfahren sah der BfDI einen grob fahrlässigen Verstoß gegen Artikel 32 Datenschutz-Grundverordnung (DSGVO) und verhängte die Millionenbuße, wogegen sich die Firma gerichtlich zur Wehr setzte.

Die DSGVO schreibt vor, dass Unternehmen geeignete technische und organisatorische Maßnahmen ergreifen müssen, um die Verarbeitung personenbezogener Daten systematisch zu schützen. 1&1 räumte den Datenschutzverstoß ein, stellte ihn aber als Einzelfall dar – und eben nicht als ein systematisches Problem. Zudem sei die von Kelber verhängte Geldbuße unverhältnismäßig hoch.

Das Gericht bestätigte in der Sache den Datenschutzverstoß. Es handele sich aber nur um einen geringen Verstoß, der nicht „zur massenhaften Herausgabe von Daten an Nichtberechtigte" habe führen können. Da die über Jahre bei 1&1 geübte Authentifizierungspraxis bis zu dem Bußgeldbescheid nicht beanstandet worden sei, habe es dort an dem notwendigen Problembewusstsein gefehlt.

Trotz abgesenkter Strafe sah sich Bundesdatenschützer Kelber durch das Urteil bestätigt. Das Gericht sei der Auffassung des BfDI in wesentlichen Punkten gefolgt. Das Urteil zeige, dass Datenschutzverstöße nicht ohne Folgen blieben: „Ich bin überzeugt, dass diese Entscheidung in den Chefetagen von Unternehmen wahrgenommen wird. Klar ist schon jetzt: Kein Unternehmen kann es sich mehr leisten den Datenschutz zu vernachlässigen" (Kannenberg, Datenschutzverstoß bei 1&1: Gericht senkt Millionenstrafe deutlich ab, www.heise.de 11.11.2020, Kurzlink: https://heise.de/-4957463).

Buchbesprechungen



Prof. Dr. Dieter Frey, LL.M. (Hrsg.)
eSport und Recht - Handbuch
2021, 388 Seiten, broschiert,
ISBN 978-3-8487-5584-4, 78 €

(ha) Insbesondere für Nicht-Juristen kann es schwierig sein sich über die rechtlichen Rahmenbedingungen im Sport und erst recht im neu und stetig wachsenden eSport-Bereich zu orientieren. Eine Vielzahl von Akteuren versucht dort mitzumischen und ihren Platz in diesem „Ökosystem" zu finden. Darauf reagiert das aktuell vorliegende Handbuch „eSport und Recht", herausgegeben von Prof. Dieter Frey mit Beiträgen von insgesamt zehn Anwältinnen und Anwälten, „als erstes juristisches Praxiswerk" durch Einordnung der „zum Teil komplexen Interaktionen und Rechtsbeziehungen".

Aufgeteilt in acht Kapitel mit insgesamt 31 (fortlaufend nummerierten) Paragrafen als Unterkapitel wird der eSport als eigene Sportart ebenso problematisiert wie die Rolle der verschiedenen Akteure, von Organisationen, Profis, Veranstaltern und Zuschauern bis zu den Medien und Werbetreibenden. Den Abschluss der 340 Text-Seiten bildet das Kapitel über Steuern. Dass in diesem Handbuch das Glossar gleich zu Beginn hinter dem Abkürzungsverzeichnis zu finden ist, irritiert deutlich weniger als

die Form der Literaturhinweise, die zu Beginn der Kapitel als Fließtext ohne Zeilenumbrüche teils über mehrere Seiten präsentiert werden und damit nahezu nicht brauchbar sind.

Über diese Irritation kann nur das Stichwortverzeichnis im Anhang hinwegtrösten, das auf 20 Seiten mit Paragrafen und Randnummern einen recht vollständigen Eindruck macht. Da hier der Aspekt des Datenschutzes und dessen Behandlung im „Praxishandbuch" im Vordergrund stehen soll, wurde der Zugang über dieses Stichwort im Stichwortverzeichnis gewählt.

Der erste Beitrag zum Datenschutz (eigenes Teilkapitel in „Rechtliche Positionen der Akteure, § 10 eSportler") lautet lapidar: „Datenschutzrechte der Spieler ... erlangen insbes. im Rahmen der medialen Auswertung einer eSport-Veranstaltung Relevanz" und dort wird auf § 22 im hinteren Teil des Handbuchs verwiesen, in dem dann aber lediglich konstatiert wird: „Bei Nichteingreifen des Medienprivilegs setzt die Zulässigkeit einer datenschutzrechtlich relevanten Verarbeitung entweder einen Erlaubnistatbestand oder eine Einwilligung des Betroffenen voraus". Offen bleibt dort, welche Erlaubnistatbestände es denn geben könnte.

Der zweite Beitrag unter der Überschrift „Arbeitnehmerdatenschutz im eSport" (§ 16 Vertragsparteien und ihre Pflichten) ist gehaltvoller. Die hier vorgetragene Position, eSport-Profis müssten in die Verarbeitung personenbezogener Daten einwilligen, kann aber zur Verwirrung führen. So wird zwar am Rande darauf hingewiesen, dass die Einwilligung freiwillig erfolgen muss, doch bleibt offen, was bei deren Rücknahme geschehen soll. Dem Vernehmen nach ist selbst unter langjährigen Datenschutzexperten streitig, ob eine Einwilligung auch dann eingeholt werden sollte, wenn – falls sie fehlt – auf andere Verarbeitungsgrundlagen zurückgegriffen werden soll, doch jedenfalls wäre eine einmal erteilte Einwilligung widerrufbar. Und in diesem Fall würde der Arbeitsvertrag als solches weiter Gültigkeit haben, ohne dass personenbezogene Daten wie beispielsweise in Ranglisten und Statistiken weiter verarbeitet werden dürften.

Ähnlich vage bleibt im § 16 auch die Problematisierung der Einwilligung im Falle von minderjährigen eSport-Profis, weil die dort getroffenen Aussagen mit „unter Umständen" und „gegebenenfalls" relativiert werden. Beispiel: „Das Ausmaß der Datenerhebung und -verarbeitung ist bei der Einholung der Einwilligung eines Minderjährigen stets zu beachten". Dem abschließenden Hinweis in diesem Kapitel, die Regelung über Verarbeitung personenbezogener Daten im Spielervertrag „so detailliert wie möglich" vorzunehmen, ist unbedingt zuzustimmen.

Insgesamt machen die allgemeinen Beiträge den Eindruck, gut und fundiert recherchiert zu sein und einen aktuellen Überblick über das gesamte „Ökosystem" des eSports zu geben. Vor allem das Kapitel 4 mit der Beleuchtung der rechtlichen Positionen der Akteure und Schwerpunkt auf dem Urheberrecht kann überzeugen und ist wirklich handbuchmäßig brauchbar.

Es fehlen aus Sicht des engagierten Hobbyspielers aber Hinweise auf die Datenschutz-Rahmenbedingungen bei kleineren, lokalen Veranstaltungen. Trotz der Hinweise im Kapitel 6 „Rechtliche Fragestellungen bei der Organisation von Wettkämpfen" zu den AGBs beim Verkauf von Zuschauer-Eintrittskarten kommt dieses Thema deutlich zu kurz, da offen bleibt, wie die dort erwähnte Datenschutzklausel aussehen könnte. Bedauerlich ist weiterhin, dass – wenngleich nicht alle Spiele auch eSport-fähig sind – auf die „Datenskandale" aus der Online-Spielewelt nicht eingegangen wird, obwohl doch gerade die Spieleherausgeber oft davon betroffen waren (Details siehe dazu DANA 4/2019, 200 ff.).

Cartoon



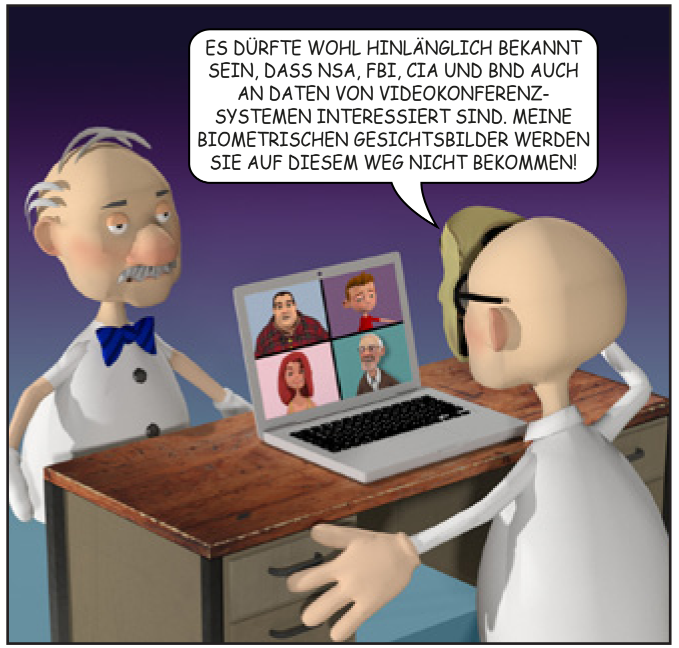




Bild: shutterstock.com/cosmin4000